EDITORIALE

TORNA IL CYBER ENIGMA

Vi siete accorti di niente? Guardate bene a pagina 32. E proprio così, è tornato il Cyber Enigma, uno degli “spazi” più popolari e rimpianti di HJ.
Abbiamo deciso di ripristinarlo, si può proprio dire, a furor di popolo. Sono state infatti tantissime le richieste che avevano generato anche un post, sul forum, in cui avevamo preannunciato questa possibilità.
Ora è ufficiale. A questo punto non vi resta che risolverlo, del resto se avete voluto la bicicletta…
Volevo anche ringraziare l’editore che ha sacrificato l’unica pagina di pubblicità, anche se interna, per accogliere questa richiesta. Ora si può dire che HJ è davvero cento per cento notizie e articoli.
Vi segnalo inoltre la terza puntata del corso in C - a proposito vi piace? – che sta entrando nel vivo e che tanto riempie di gioia il nostro grafico in fase di impaginazione, tra codici e box da collocare con rigida disposizione.
Piccola nota a margine: stiamo ricevendo davvero molte e-mail. Cerchiamo di rispondere a tutti, in alcuni periodi, concomitanti con la chiusura della rivista, siamo meno presenti in fase di risposta, ma leggiamo davvero tutto. Quindi scriveteci perché per noi è importante conoscere la vostra opinione. Sempre.

Altair

laboratorio@hackerjournal.it
Questo indirizzo è stato creato per inviare articoli, codici, spunti e idee. E’ quindi proprio una sorta di ”incubatore di idee”.

posta@hackerjournal.it
E’ l’account creato per l’omonima rubrica che è ricomparsa nelle pagine della rivista. A questo indirizzo dovete inviare tutte le mail che volete vengano pubblicate su HJ.

redazione@hackerjournal.it
Questo è l’indirizzo canonico. Quello con cui potete avere un filo diretto, sempre, con la redazione, per qualsiasi motivo che non rientri nelle due precedenti categorie di posta.

Sommario

Copertina: Daniela Festa ldfesta@libero.it

Anno 10 - N.202
27 maggio / 9 giugno 2010

Editore (sede legale)
WLF Publishing S.r.l.
Socio Unico Medi & Son S.r.l.
via Donatello 71 - 00196 Roma
Fax 063214606

Realizzazione editoriale
Progetti e promozioni Srl
redazione@progettiepromozioni.com

Printing
Grafiche Mazzucchelli S.p.a - Seriate (BG)

Distributore
M-DIS Distributore SPA
via Cazzaniga 2 - 20123 Milano

Hacker Journal
Pubblicazione quattordicinale registrata al Tribunale di Milano il 27/10/03 con il numero 601.
Una copia: 2,00 euro

Direttore Responsabile
Teresa Carsaniga
redazione@hackerjournal.it

WLF Publishing S.r.l. - Socio Unico Medi & Son S.r.l. è titolare esclusivo di tutti i diritti di pubblicazione. Per i diritti di riproduzione, l’Editore si dichiara pienamente disponibile a regolare eventuali spettanze per quelle immagini di cui non sia stato possibile reperire la fonte.

Gli articoli contenuti in Hacker Journal hanno scopo prettamente divulgativo. L’Editore declina ogni responsabilità circa l’uso improprio delle tecniche che vengono descritte al suo interno. L’invio di immagini ne autorizza implicitamente la pubblicazione anche non della WLF Publishing S.r.l. - Socio Unico Medi & Son S.r.l.

Copyright WLF Publishing S.r.l.
Tutti i contenuti sono protetti da licenza Creative Commons Attribuzione-Non commerciale-Non opere derivate 2.5 Italia: creativecommons.org/licenses/by-nc-nd/2.5/it

Informativa e Consenso in materia di trattamento dei dati personali (Codice Privacy d.lgs. 196/03)
Nel vigore del d.lgs. 196/03 il Titolare del trattamento dei dati personali, ex art. 28 d.lgs. 196/03 è WLF Publishing S.r.l. - Socio Unico Medi & Son S.r.l. (di seguito anche “Società”, e/o “WLF Publishing”), con sede in via Donatello 71 Roma. La stessa La informa che i Suoi dati verranno raccolti, trattati e conservati nel rispetto del decreto legislativo ora enunciato anche per attività connesse all’azienda. La avvisiamo, inoltre, che i Suoi dati potranno essere comunicati e/o trattati nel vigore della Legge, anche all’estero, da società e/o persone che prestano servizi in favore della Società. In ogni momento Lei potrà chiedere la modifica, la correzione e/o cancellazione dei Suoi dati ovvero esercitare tutti i diritti previsti dagli artt. 7 e ss. del d.lgs 196/03 mediante comunicazione scritta alla WLF Publishing S.r.l. e/o al personale Incaricato preposto al trattamento dei dati. La lettura della presente informativa deve intendersi quale consenso espresso al trattamento dei dati personali.

SICUREZZA: È UNA QUESTIONE DI SKILL

L'altro giorno mi sono recato nel mio istituto di credito e, facendo una scansione col telefonino, ho scoperto con mio grande stupore che la rete Wi-fi interna era accessibile a chiunque. Ottimo perché nell'attesa ho letto le notizie on-line, scaricato mail e altre attività senza gravare sulla flat (non illimitata) della mia tariffa dati.
Stupito ho segnalato la cosa al mio interlocutore, il responsabile dell'ufficio fondi e investimenti con cui avevo un appuntamento. Mi è parso che gliene importasse davvero poco, comunque ha manifestato un genuino stupore, snocciolato un discorso di circostanza, anche piuttosto accorato, dopodichè è passato immediatamente alla presentazione delle "opportunità di investimento" accantonando, credo per sempre, il problema.
Il paradosso risulterà evidente anche ai meno attenti: mi parlano di investimenti sicuri ed è come se avessero un cavo tirato fino al giardino antistante da cui tutti possono collegarsi e accedere alla rete interna...
Il rischio del Wirelles è proprio questo. Non si vede ed è sottovalutato dagli amministratori di sistema (d'accordo il caso in questione è davvero paradossale, ma non isolato), E' evidente che un cavo Ethernet penzolante fuori da una finestra della banca darebbe più preoccupazione, ma il discorso di fondo non cambia. Volendo generalizzare ulteriormente, spesso il problema della sicurezza affonda le sue radici in un atteggiamento poco attento del personale IT. Si tratta a volte di disattenzione, di superficialità, o di un skill non adeguato. I maggiori rischi di intrusione affondano proprio nella umane debolezze. Inutile prendersela col software o l'hardware. Sono solo degli strumenti. E' l'elemento umano che determina vittorie e sconfitte. Lo è stato fin dagli albori dei tempi quando la civiltà umana si confrontava in battaglie decisamente più cruente e lo sarà ancora per molto tempo a venire.
Nel frattempo ho sottoscritto dei buoni fruttiferi alla posta sotto casa. Hanno una WLAN protetta con chiave WPA. Se il buongiorno si vede dal mattino...

NeWS

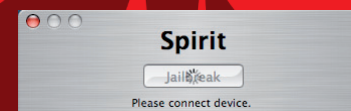
Eugene Kaspersky è CEO of the Year

Il co-fondatore e CEO di Kaspersky Lab, Eugene Kaspersky, è stato premiato come il miglior CEO dell'Anno. Il riconoscimento è stato conferito dal prestigioso SC Awards Europe 2010 a Londra.
Eugene Kaspersky si è detto onorato di accettare il premio tra gli applausi di centinaia di professionisti della sicurezza IT presenti alla cerimonia, organizzata dalla testata inglese, SC Magazine, al Wyndham Grand London Chelsea Harbour.
Gli SC Awards Europe 2010 sono un appuntamento molto importante per tutti gli operatori del settore della sicurezza IT e premiano l'impegno e l'eccellenza dimostrata durante tutto l'anno. Commentando il premio, Eugene Kaspersky ha affermato: "Sono veramente onorato che la qualità del lavoro ed i significativi progressi compiuti dai nostri team di tutto il mondo siano stati riconosciuti qui a Londra. Il successo di Kaspersky Lab si fonda sul duro lavoro e sulla determinazione per rendere il mondo un luogo sicuro. Guidare questa azienda è per me un privilegio".
Il CEO of the Year Award è l'ultimo riconoscimento che Eugene Kaspersky ha ricevuto negli ultimi dodici mesi, riconoscendo la crescita di Kaspersky Lab in tredici anni di attività.
Oggi Kaspersky Lab è uno dei primi quattro fornitori di soluzioni di sicurezza IT al mondo per utenti endpoint. Un team di 1700 persone che lavorano instancabilmente in 100 paesi per proteggere oltre 300 milioni di utenti IT in tutto il mondo.
Il 28 aprile 2010 a Londra, Eugene Kaspersky sarà inserito nella Infosecurity Europe 2010 Hall of Fame, un riconoscimento per il suo contributo al progresso del settore della sicurezza IT da oltre venti anni. Sarà affiancato da Lord Erroll di Merlin; Stephen Bonner, Managing Director Information Risk Management di Barclays ed Edward Gibson, Director - Forensics Technology Services di PricewaterhouseCoopers.

APPLE VS ADOBE

Secondo il New York Post, Apple potrebbe essere oggetto di indagine antitrust da parte del Dipartimento della Giustizia statunitense (DOJ) e della Federal Trade Commission (FTC) per modifiche apportate alla versione 3.3.1 del proprio iPhone SDK 4.
La questione è stata sollevata dalle polemiche innescate dalla decisione di Apple di bandire, con l'introduzione del nuovo SDK 4 e degli strumenti di sviluppo correlati, le applicazioni crossplatform in Flash realizzate con Adobe CS 5.
La "lite" tra i due contendenti, Adobe e Apple, ha attirato l'attenzione dei media e delle autorità preposte su un fatto che è ormai da tempo acclarato: il sistema di vendita dell' applicazione attraverso Apple Store, come abbiamo avuto modo di scrivere qualche tempo fa proprio su HJ, è un sistema "meravigliosamente" chiuso, da sempre, per nulla o poco permeabile all'ingresso di terze parti. Apple ha inventato questa forma di business e ora se la tiene ben stretta. Tutto sommato è anche comprensibile...

Jailbreak per iPad

E' stato rilasciato un pacchetto in grado di effettuare il jailbreak dell'iPad e dei più recenti iPhone OS, permettendo agli utenti di installare centinaia di applicazioni non approvate, o per meglio dire non pubblicate su Apple Store sul proprio dispositivo Apple.
Il pacchetto, chiamato Spirit , effettua il jailbreaks di tutti gli iPad, iPod touch o iPhone con sistema operativo OS 3.1.2, 3.1.3 e 3.2.
Per essere installato richiede una versione di iTunes 9 (compresi 9.1.1). E' disponibile una versione per Windows e una per Mac di Spirit, entrambe scaricabili all'indirizzo: http://spiritjb.com.

Microsoft ritira la patch inutile

Dopo aver rilasciato la patch MS10-025, Microsoft, si è apprestata a ritirarla in tutta fretta. L'aggiornamento era destinato agli utenti di Windows 2000 Server che eseguono Windows Media Service, per sistemare una falla classificata critica.
In seguito però la stessa Microsoft si è accorta che la patch non risolveva il problema e ha provveduto a ritirarla.
Ora Microsoft ha ritirato l'aggiornamento poiché si è accorta che la correzione non risolveva il problema. Ora si è in attesa del rilascio del nuovo aggiornamento che dovrebbe essere già disponibile sul sito nel momento in cui questo giornale sarà distribuito in edicola.
Per monitorare la situazione si può fare riferimento all'indirizzo http://www.microsoft.com/technet/security/bulletin/ms10-025.mspx.

McAfee

McAfee cancella un file di sistema

Un aggiornamento del software di sicurezza di McAfee ha creato un falso positivo bloccando i sistemi operaitivi Windows Xp di migliaia di computer. Il problema è stato creato dal rilascio di un update difettoso (il 5958 DAT) che ha scambiato erroneamente uno dei componenti di Windows XP, il file svchost.exe, per il virus W32/Wecorl.a eliminandolo così dal sistema.
Secondo le dichiarazioni ufficiali, è stato coinvolto lo 0,5% degli account enterprise globali e una frazione ancora minore degli utenti domestici. Si tratta comunque di diverse migliaia di utenti e di un danno di immagine per McAfee non indifferente.
La società dal canto suo ha bloccato il DAT difettoso dopo quattro ore dal suo rilascio, troppo tardi per molti utenti. MacAfee sul suo sito, all'indirizzo www.mcafee.com/it/about/false_positive_response.html ha subito pubblicato il seguente messaggio:

"Alcuni clienti che usano Window XP hanno incontrato dei problemi in conseguenza di un DAT File difettoso rilasciato all'inizio di questa settimana alle ore 14.00 di mercoledì 21 aprile.
La nostra priorità è di farvi ripristinare la funzionalità ed operatività del vostro computer qualora fosse stato danneggiato o reso inoperativo a causa di questo DAT File difettoso. Per questo motivo McAfee sta prendendo tutte le misure preventive possibili affinché questo non avvenga di nuovo".

Allo stesso indirizzo vengono fornite le indicazioni, sia per gli utenti privati che per quelli aziendali, per risolvere il problema.

Twitter chiude al P2P

Due account Twitter relativi a due siti crocevia per file torrent sono stati bloccati e oscurati alla vista di tutti i follower. Nel motivare la decisione i responsabili di Twitter hanno parlato solamente di abuso dei termini di servizio: entrambi i siti bloccati fornivano infatti regolarmente informazioni relative al traffico di torrent.
Nonostante gli addetti ai lavori sospettino che dietro a questo provvedimento ci sia una questione di copyright, in realtà i due account formalmente avrebbero violato le regole di Twitter che stabiliscono espressamente che qualora il flusso di messaggi contenga una quantità eccessiva di link l'account possa essere sospeso.
Lo scorso febbraio decine di migliaia di utenti di Twitter si erano visti resettare la propria password per contrastare quello che si temeva essere uno scam organizzato su vasta scala per colpire tramite gli account Twitter.

eScan Antivirus Toolkit Free

E' finalmente disponbile la versione gratuita di eScan Antivirus Toolkit (versione 12.x) che, rispetto alla release precedente che forniva solo l'opzione di scansione del sistema, questa nuova versione consente anche di rimuovere eventuali infezioni provocate da virus, spyware, adware e ogni altro tipo di malware.

"L'applicazione FREE MWAV Toolkit Utility è stata sempre molto apprezzata dagli utenti in quanto un ottimo strumento per la scansione del PC che è possibile avviare senza alcuna installazione" afferma Govind Rammurthy (CEO e Managing Director di MicroWorld) "Coerentemente alla strategia aziendale, finalizzata a consolidare il posizionamento del nostro brand, abbiamo scelto di unificare tutta la nostra offerta sotto il marchio eScan. Per questo abbiamo rinominato MWAV Toolkit Utility con la dicitura eScan Antivirus Toolkit Utility. Inoltre, per rispondere alle richieste provenienti da clienti e partner, abbiamo deciso di fornire, con questa nuova versione, l'opzione per la pulizia dei malware. Oggi gli utenti di eScan Antivirus Toolkit possono quindi usufruire non solo dell'eccellente funzione di scansione, ma anche contare sulle performance di pulizia di eScan che ha riscosso numerosi riconoscimenti internazionali. Non solo: è anche possibile programmare la scansione automatica all'avvio del sistema aggiungendo eScan Antivirus Toolkit alla lista dei programmi da eseguire all'avvio di Windows".

eScan Antivirus Toolkit (era conosciuto fino a questo momento come MWAV Toolkit Utility) non richiede installazione e può essere avviato direttamente dall'hard disk del computer, tramite USB drive o dal CD ROM, anche in presenza di un software antivirus precedentemente installato nel PC.

eScan Antivirus Toolkit viene inoltre aggiornato ogni giorno così da individuare i più recenti spyware e adware rilasciati, e pulire velocemente ogni nuova minaccia diffusa nella rete. La compatibilità è assicurata con Microsoft Windows Vista, Windows 7 e 2008 (32 e 64 bit).

Il download è effettuabile da http://www.escanav.com/english/content/products/MWAV/escan_mwav.asp

Ricordo Meggiato
redazione@hackerjournal.it

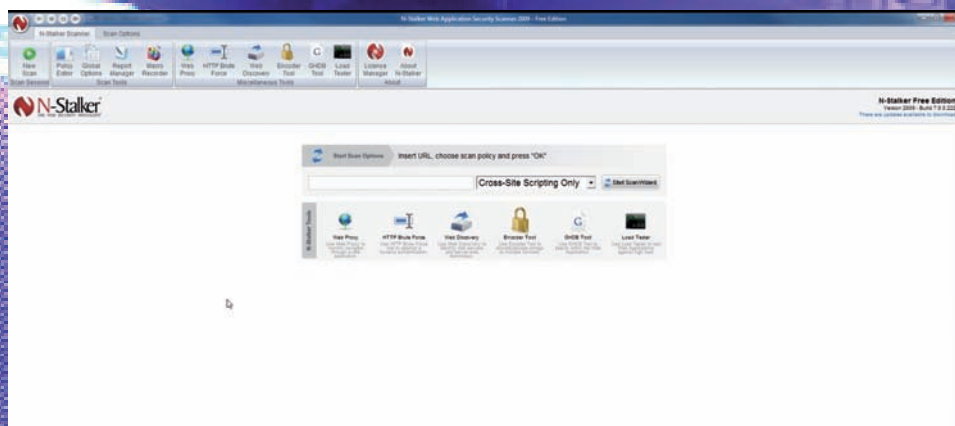
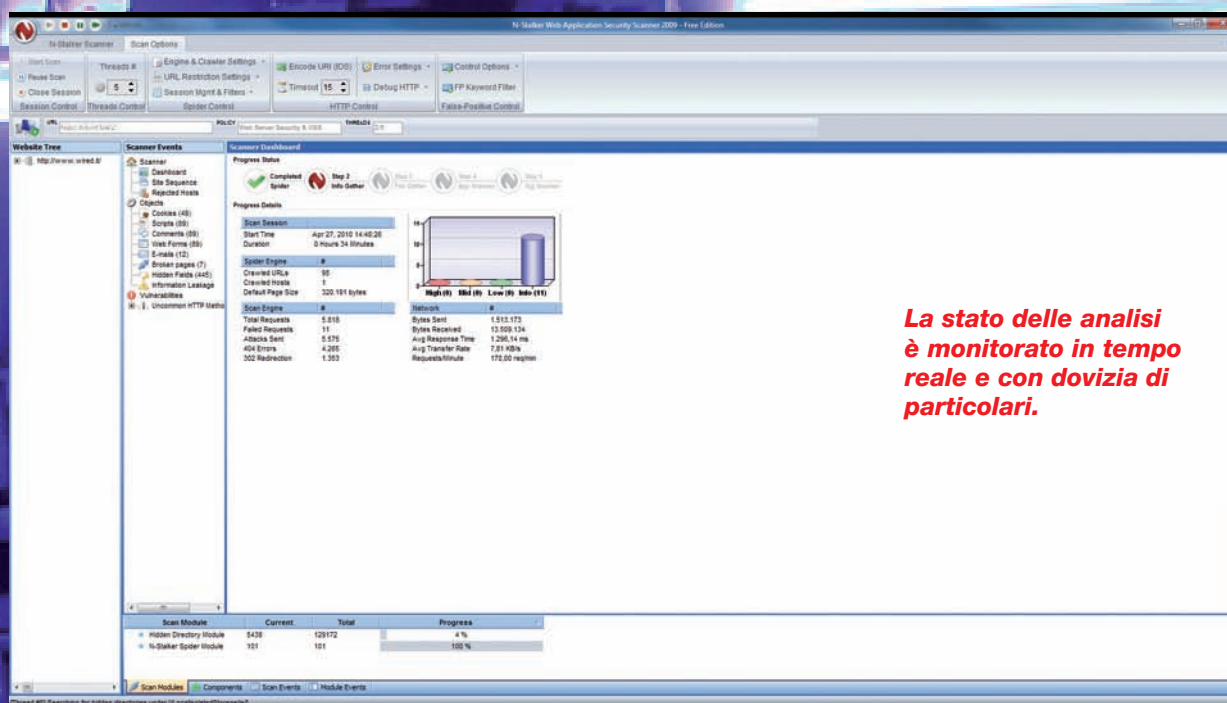
A CACCIA D'INVULNERABILITÀ

MONITORING E CHI L'HA DETTO CHE TROVARE FALLE NEI WEB-SERVER SIA UNA PROCEDURA LUNGA E NOIOSA?

L'azione di qualsiasi hacker è preceduta da una fase di analisi del proprio obiettivo. Un po' come avviene in una partita di calcio, dove una squadra rileva i punti deboli dell'altra, anche nel campo della sicurezza informatica c'è bisogno di verificare dove si può agire. E questo, sul versante opposto, è quanto dovrebbe fare chi tiene sotto controllo la sicurezza di un sito. Il secondo, tuttavia, non è sempre mosso dalla voglia di conoscenza del primo, e preferisce rivolgersi a software belli e pronti che svolgano il lavoro sporco in completa autonomia (o quasi). Si tratta di programmi molto costosi e, nella maggior parte dei casi, chiusi. E a volte pure capaci di violare l'etica hacker, anche se questo non significa che non possano tornare utili proprio... agli hacker. Tra questi c'è N-Stalker, web-scanner che non ha certo bisogno di presentazioni e che, forte di un'interfaccia gradevole, dispone di un discreto armamentario di funzioni in grado di rilevare le più recenti vulnerabilità dei web-server. Noto anche per un prezzo tutt'altro che abbordabile (si parte da circa 270 €), da qualche tempo N-Stalker è disponibile anche in una versione totalmente gratuita. Ovviamente c'è qualche limitazione rispetto alle edizioni commerciali, ma la dotazione di base val bene una prova.

INSTALLAZIONE IN POCHI CLIC

N-Stalker Free Edition è disponibile all'indirizzo nstalker.com/products/free. Una volta qui, si clicca in basso a sinistra, su Click to download Free Version, e si compila il modulo online. Nessuno ci obbliga a inserire dei dati veri, ma l'indirizzo di posta elettronica deve essere quanto meno "raggiungibile". Infine si clicca su Send e si va all'indirizzo e-mail specificato, dove si trova il link da cui scaricare

Alcuni degli strumenti a disposizione di N-Stalker. Come possiamo vedere, non solo analisi...

La stato delle analisi è monitorato in tempo reale e con dovizia di particolari.

l'applicazione, che sta in un file di circa 13 MB. Effettuato il download, non resta che fare doppio clic sul file e procedere con la semplice installazione, e avviare N-Stalker Free Edition. All'avvio, il programma si occupa di verificare la presenza di aggiornamenti (se disponibili è bene installarli subito) e, in capo a pochi istanti, ci mette di fronte alla sua interfaccia principale.
Utilizzare questo software è molto semplice, se non abbiamo particolari esigenze: digitiamo l'indirizzo del web-server da controllare, nella finestrella centrale, e poi utilizziamo il menu a tendina, che si trova in parte, per selezionare il tipo di controllo. Ce ne sono cinque diversi, ciascuno preposto a un'analisi specifica. Una volta selezionato questo parametro, non ci resta che cliccare su Start Scan Wizard. Si avvia uno wizard, cioè una procedura guidata alla scansione del sito. Nella prima finestra possiamo caricare i parametri di una scansione precedente o di uno spider, oppure passare oltre, cliccando direttamente su Next. A questo punto la finestra di ottimizzazione, Optimizing Settings, consente un'ultima ottimizzazione del processo di analisi, effettuabile cliccando su Optimize. In questo caso, N-Stalker esegue una serie di test per modificare al meglio i parametri di controllo. Anche a basso livello, cliccando su Scan Settings. Quando tutti i parametri sono configurati, clicchiamo su Next, rivediamo le impostazioni scelte e, per procedere con la vera scansione, clicchiamo su Start Session.
Un avviso ci ricorda che la versione Free Edition si limita all'analisi delle prime cento pagine del sito desiderato: più che sufficienti per una buona prova sul campo! Per finire, una volta arrivati alla pagina della scansione, clicchiamo su Start Scan, in alto a sinistra, e osserviamo l'avanzare della scansione.
Dopo qualche minuto (ma il tempo è variabile in base alla velocità della nostra connessione e agli esiti dei test), compare una finestra che ci dà la possibilità di salvare i risultati dell'analisi, che sono poi mostrati in tutto il loro splendore.
Numero di pagine esaminate, vulnerabilità trovate, cookie e indirizzi e-mail presenti, sono solo alcune delle prelibatezze elargite da N-Stalker Free Edition. Il quale non limita alla sola analisi le sue possibilità. Per esempio, dalla pagina iniziale possiamo selezionare anche l'http Brute Force, un potente e completo strumento in grado di eseguire semplici, ma efficaci, attacchini forza bruta. Con la possibilità di caricare file di testo che elencano nomi utente e password, o specificare particolari espressioni di autenticazione.
Al di là delle funzionalità, estese ed entusiasmanti, di un software molto diffuso in ambito professionale e finalmente disponibile in una versione gratuita, N-Stalker si fa apprezzare anche per le prestazioni. La velocità di scansione, considerate le analisi approfondite effettuate, è elevata e consente di farsi in pochi minuti una precisa idea sui punti deboli di un web-server. A quel punto, forti di queste informazioni, agire, "in un senso o nell'altro", è molto più semplice.

Massimiliano Rinaldi
redazione@hackerjournal.it

ABC DELLE PORTE SU MAC OSX

PORT SCAN

SIETE SICURI CHE QUALCUNO NON ABBIA APERTO UNA PORTA PERICOLOSA NEL VOSTRO MAC E SIA LÌ, IN ASCOLTO? SE VOLETE SGOMBRARE IL CAMPO DA OGNI SOSPETTO QUESTA È LA MINI GUIDA CHE FA PER VOI.

Quando si parla di sicurezza legata al Mac i più fanno spallucce. Del resto i computer di casa Apple vuoi per la loro poca diffusione (per esser generosi) vuoi per un'architettura del sistema operativo decisamente solida, sono da sempre considerati quasi invulnerabili.
Eppure anche il Mac è esposto a rischi. Per comunicare con l'esterno deve aprire dei canali di comunicazione, delle porte, attraverso le quali possono intrufolarsi pericolosi intrusi. Internet è composto da client e server.

CLIENT E SERVER

Il client ricerca alcune informazioni da Internet che si trovano su un server. Un client utilizza un'applicazione per navigare in Internet. Tutti i computer che sono collegati a Internet hanno un indirizzo IP. L'indirizzo IP serve come principale indirizzo per la macchina. Ogni servizio sul sistema ha un identificatore univoco chiamato porta. Una porta è un numero univoco tra 0 e 65535. Un elenco delle porte è disponibile su ogni sistema Mac OS X, nel file / etc / services. Le porte comprese tra 0 e 1023 sono denominate "well-know ports." (porte conosciute) Un piccolo programma che viene eseguito sul computer, chiamato demone, rileva ogni servizio disponibile su un computer. Il demone si lancia e si lega a una porta specifica, quindi aspetta in ascolto per le connessioni attraverso quella porta. Quando una connessione è aperta verso quella porta, il demone si sveglia e invia una risposta al client.

LE PIÙ POPOLARI

Forse, la porta 80 è la porta più "conosciuta". È infatti la porta più spesso utilizzata per HTTP, che è il traffico Web. Quando si digita l'indirizzo www.apple.com nel proprio browser Web, il browser prima esegue una ricerca DNS, quindi invia una richiesta all'indirizzo IP del server, sulla porta 80. Tuttavia, a volte il proprio browser viene reindirizzato a un'altra porta. La più comune è la pagina https sulla porta 443 (secure HTTP), che viene utilizzata per acquisti online, banche, e così via. Altre porte popolari sono la 25, utilizzata per il Simple Mail Transfer Protocol (SMTP), che gestisce l'invio di e-mail; la 110 POP (Post

Office Protocol), che è utilizzato per verificare la posta elettronica; la 143 IMAP (Interactive Mail Access Protocol) , che è un'alternativa al POP per il controllo e-mail; la 21, utilizzata per FTP, e 22, utilizzata per ssh (Secure Shell).
TCP / IP non determina quali porte vengono utilizzate per le specifiche applicazioni. È possibile gestire un server Web su qualsiasi porta desiderata.
La porta 8080 è popolare per essere la porta di default per il server Web Apache. Il sistema di porte "well-know ports" è fornito per aiutare l'utente e rendere questo tipo di configurazione più semplice. Cosi come i server DNS aiutano nella traduzione di indirizzi IP numerici complessi, difficili da ricordare, in nomi molto più semplici e memorizzabili nella traduzione, anche le porte "conosciute" servono di base per la standardizzazione. Invece di dover chiedere a quale porta effettuare la connessione per ogni singolo sito Web, si può semplicemente accettare di utilizzare la porta 80 per il server Web.

MONITORARE LE PORTE APERTE

È bene eseguire un controllo sul proprio sistema ogni volta che si installa o si aggiorna ogni tipo di servizio per garantire che si aprano solo le porte che si desidera avere aperte. Il modo per farlo è di eseguire un software di scansione delle porte. I port scanner sono un importante strumento per l'arsenale di un hacker. Eseguendo un port scan, si può vedere che cosa il vostro computer offre in termini di porte disponibili e quindi consente di utilizzare tali aperture per penetrare il vostro sistema.
Eseguendo un port scan del vostro computer, si potrà sapere quello che anche gli hacker sanno, e chiudere qualsiasi involontaria apertura.
Per verificare quali porte sono aperte sul proprio sistema, è consigliabile eseguire un software di terze parti, perché Apple ha fornito Utility Network ma il uso utilizzo non è del tutto esauriente e quindi soddisfacente. Come la maggior parte delle cose per quanto riguarda l'interazione con Unix in Mac OS X, si avrà la scelta tra l'utilizzo di un' interfaccia grafica o una riga di comando.
Se siete curiosi e volete proprio provare, Apple, come già detto, fornisce un'applicazione nella cartella Utility, all'interno della cartella Applicazioni, chiamata Utility Network, che dispone di un rudimentale port scan. Per accedere al port scan, lanciare l'applicazione e fare clic sulla scheda Porte nella barra in alto.
Per una rapida correzione e chiusura delle porte involontariamente aperte, è possibile utilizzare un servizio on-line che segue la scansione delle porte del computer dall'esterno.
Il servizio è fornito da Gibson Research Corporation, un produttore di software di sicurezza per i sistemi Windows ed è raggiungibile cliccando su ShieldsUP! Dal link da www.grc.com.
La cosa migliore è tuttavia utilizzare un software installato sul proprio computer, comunque questa soluzione online fornisce una buona panoramica della situazione generale del vostro computer, limitatamente alle porte utilizzate e aperte.

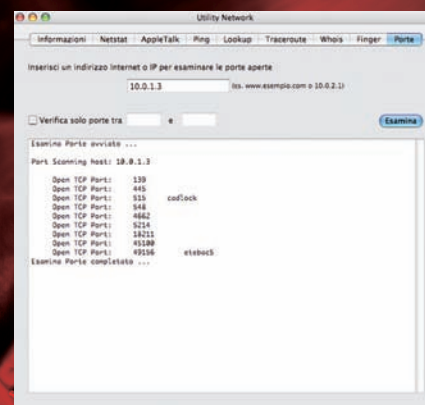
PROGRAMMI DI VERIFICA A INTERFACCIA GRAFICA

Diversi programmi di terze parti sono disponibili per mostrare i demoni in esecuzione e su quali porte sono in ascolto. Ecco un breve elenco degli strumenti più popolari:

AysMon (Are You Serving Monitor) è un programma scritto in Java ed è disponibile all'indirizzo www.pepsan.com/aysmon/index.html. È distribuito come un file disco immagine.
Per montare l'immagine, è sufficiente fare doppio clic sull'icona .dmg del file e quindi trascinare la cartella AysMon nella cartella Applicazioni.
AysMon viene fornito con un elenco di servizi, controlla il vostro computer per ciascuno di essi, e vi mostra i risultati. AysMon è shareware e costa 5 dollari.
WhatPorts / 1,1 è un dispostivo di esplorazione delle porte freeware disponibile all'indirizzo: www.davtri.com / index.py / freeware.

Porte "note" TCP e UDP utilizzate da prodotti software Apple.
Apple ha ufficialmente rilasciato questo elenco di porte abitualmente utilizzate dai prodotti Apple, non si tratta evidentemente di un elenco completo ma solo orientativo, ci sono infatti software non proprietari (ad esempio di P2P) che sfruttano altre porte.

TUTTO IL TRAFFICO SOTTO ESAME

Il nostro Mac sottoposto all'esame delle Porte con Utility Network (Applicazioni>Utility> Utility Network) presenta una serie di porta "note" da 139 a 548. E poi una serie di porte aperte "sospette".
Il risultato della scansione delle porte aperte del Mac con Utility Network

La 45100 è una porta di comunicazione aperta da Limeware che è in effetti in uso.

La 4662 è utilizzata da aMule, anch'esso in uso.

La 5214 è una porta aperta da un file Torrent (in effetti attivo).
Così come la 49156 che viene utilizzata come BitTorrent client.

Infine la porta 18211 è una porta di ascolto del Firewall.

Porta	TCP o UDP	Nome servizio o protocollo	RFC	Utilizzato da/Informazioni aggiuntive
7	TCP/UDP	echo	792	–
20	TCP	File Transport Protocol (FTP)	959	–
21	TCP	Controllo FTP	959	–
22	TCP	Secure Shell (SSH)	4250 – 4254	–
23	TCP	Telnet	854	–
25	TCP	Simple Mail Transfer Protocol (SMTP)	5321	Mail (per le e-mail in uscita); MobileMe Mail (in uscita)
53	TCP/UDP	Domain Name System (DNS)	1034	MacDNS
67	UDP	Bootstrap Protocol Server (BootP, bootps)	951	NetBoot via DHCP
68	UDP	Bootstrap Protocol Client (bootpc)	951	NetBoot via DHCP
69	UDP	Trivial File Transfer Protocol (TFTP)	1350	–
79	TCP	Finger	1288	–
80	TCP	Hypertext Transfer Protocol (HTTP)	2616	World Wide Web, MobileMe, Sherlock, QuickTime Installer, iTunes Store e Radio, Software Update, RAID Admin, Backup, pubblicazione calendari iCal, iWeb, pubblicazione della galleria web MobileMe, WebDAV (iDisk), Final Cut Server
88	TCP	Kerberos	4120	–
106	TCP	Password Server (utilizzo non registrato)	–	Server password Mac OS X Server
110	TCP	Post Office Protocol (POP3) Authenticated Post Office Protocol (APOP)	1939	Mail (per le e-mail in entrata)
111	TCP/UDP	Remote Procedure Call (RPC)	1057, 1831	Portmap (sunrpc)
113	TCP	Protocollo di identificazione	1413	–
115	TCP	Secure File Transfer Program (SFTP)	913	**Nota:** alcune autorità citano questa porta come "Simple File Transport Protocol" o "Secured File Transport Protocol".
119	TCP	Network News Transfer Protocol (NNTP)	3977	Utilizzato dalle applicazioni che leggono newsgroup.
123	TCP/UDP	Network Time Protocol (NTP)	1305	Preferenze data e ora. Utilizzato per la sincronizzazione dell'ora tra i server del network.
137	UDP	Windows Internet Naming Service (WINS)	–	–
138	UDP	NETBIOS Datagram Service	–	Windows Datagram Service, Windows Network Neighborhood
139	TCP	Server Message Block (SMB)	–	Utilizzato dai servizi file e stampa Microsoft Windows, come Windows Sharing in Mac OS X.
143	TCP	Internet Message Access Protocol (IMAP)	3501	Mail (per le e-mail in entrata); MobileMe Mail (IMAP)
161	UDP	Simple Network Management Protocol (SNMP)	1157	–
192	UDP	–	–	Stato o individuazione PPP base AirPort (alcune configurazioni), Utility Amministrazione AirPort, AirPort Express Assistant
311	TCP	Server Admin, Workgroup Manager, Server Monitor, Xsan Admin	–	Amministrazione server remoto
389	TCP	Lightweight Directory Access Protocol (LDAP)	4511	Utilizzato da applicazioni che consultano indirizzi, come Mail e Rubrica Indirizzi.
427	TCP/UDP	Service Location Protocol (SLP)	2608	Browser network
443	TCP	Secure Sockets Layer (SSL o "HTTPS")	–	Siti Web protetti, iTunes Store, MobileMe (autenticazione e MobileMe Sync)
445	TCP	Server di dominio Microsoft SMB	–	–
497	TCP/UDP	Dantz Retrospect	–	–
500	UDP	ISAKMP/IKE	–	Servizio VPN con Mac OS X Server, Torna al mio Mac (MobileMe, Mac OS X v10.5 o versione successiva).
514	TCP	shell	–	–
514	UDP	Syslog	–	–
515	TCP	Line Printer (LPR), Line Printer Daemon (LPD)	–	Utilizzato per la stampa su una stampante di rete, Condivisione stampante in Mac OS X.
532	TCP	netnews	–	–
548	TCP	Apple Filing Protocol (AFP) su TCP	–	AppleShare, Personal File Sharing, Apple File Service
554	TCP/UDP	Real Time Streaming Protocol (RTSP)	2326	QuickTime Streaming Server (QTSS), lettori multimediali in streaming
587	TCP	Invio di messaggi per Mail (SMTP autenticato)	4409	Mail (per le e-mail in uscita), MobileMe Mail (autenticazione SMTP)
600–1023	TCP/UDP	Servizi Mac OS X	–	Utilizzato, ad esempio, da NetInfo. basati su RPC
623	UDP	Lights-Out-Monitoring	–	Utilizzato dalla funzionalità Lights-Out-Monitoring (LOM) di Intel Xserves; utilizzato da Server Monitor
625	TCP	Directory Service Proxy (DSProxy) (utilizzo non registrato)	–	DirectoryService, Open Directory Assistant, Workgroup Manager. **Nota**: questa porta è registrata su DEC DLM.
626	TCP	AppleShare Imap Admin (ASIA)	–	IMAP Administration (Mac OS X Server 10.2.8 o versioni precedenti, AppleShare IP 6)
626	UDP	serialnumberd (utilizzo non registrato)	–	Registrazione numero di serie server (Xsan, Mac OS X Server 10.3 e versioni successive)
631	TCP	Internet Printing Protocol (IPP)	2910	Condivisione stampante Mac OS X
636	TCP	Secure LDAP	–	–
660	TCP	Amministrazione Server MacOS	–	Server Admin (AppleShare IP e Mac OS X Server), Impostazioni del server
687	TCP	Aggiunta Admin server agli utilizzi	–	–
749	TCP/UDP	Kerberos 5 admin/changepw	–	–
985	TCP	Porta statica NetInfo	–	–
993	TCP	Posta IMAP SSL	–	MobileMe Mail (SSL IMAP)
995	TCP/UDP	Posta POP SSL	–	–
1085	TCP/UDP	WebObjects	–	–
1099 e 8043	TCP	Accesso RMI e IIOP remoto a JBOSS	–	–
1220	TCP	QT Server Admin	–	Utilizzato per l'amministrazione di QuickTime Streaming Server.

1649	TCP	IP Failover	–	–
1701	UDP	L2TP	–	Servizio VPN con Mac OS X Server
1723	TCP	PPTP	–	Servizio VPN con Mac OS X Server
2049	TCP/UDP	Network File System (NFS) (versione 3)	1094	–
2236	TCP	Macintosh Manager (utilizzo non registrato)	–	Macintosh Manager
2336	TCP	Portable Home Directories		–
3004	TCP	iSync	–	–
3031	TCP/UDP	Remote AppleEvents	–	Program Linking, Remote Apple Events
3283	TCP/UDP	Net Assistant	–	Apple Remote Desktop 2.0 o versioni successive (funzione Reporting)
3306	TCP	MySQL	–	–
3632	TCP	Compilatore distribuito	–	–
3659	TCP/UDP	Simple Authentication and Security Layer (SASL)	–	Server password Mac OS X Server
3689	TCP	Digital Audio Access Protocol (DAAP)	–	Condivisione musica iTunes
4111	TCP	XGrid	–	–
4500	UDP	IKE NAT Traversal	–	Servizio VPN con Mac OS X Server, Torna al mio Mac (MobileMe, Mac OS X v10.5 o versione successiva). **Nota**: VPN e MobileMe non possono essere configurati contemporaneamente tramite un punto di accesso Apple (come una base AirPort); MobileMe esclude VPN.
49152 65535	TCP	Xsan	–	Xsan Filesystem Access
5003	TCP	FileMaker – assegnazione nome e trasporto	–	–
5009	TCP	(utilizzo non registrato)	–	Utility Amministrazione AirPort, AirPort Express Assistant
5060	UDP	Session Initiation Protocol (SIP)	3261	iChat
5100	TCP	–	–	Condivisione fotocamera e scanner Mac OS X
5190	TCP/UDP	America Online (DSL)	–	iChat e AOL Instant Messenger, trasferimento file
5222	TCP	XMPP (Jabber)	3920	Messaggi iChat e Jabber
5223 (vedi nota 9)	TCP	XMPP over SSL	–	MobileMe (notifiche di sincronizzazione automatica)
5269	TCP	Comunicazione XMPP server-to-server	3920	Server iChat
5297	TCP	–	–	iChat (traffico locale), Bonjour
5298	TCP/UDP	–	–	iChat (traffico locale), Bonjour
5353	UDP	Multicast DNS (MDNS)	–	Bonjour (mDNSResponder)
5354	TCP	Multicast DNS Responder	–	Torna al mio Mac
5432	TCP	Database ARD 2.0	–	–
5678	UDP	Server SNATMAP	–	Il servizio SNATMAP sulla porta 5678 viene utilizzato per determinare l'indirizzo Internet esterno degli host, in modo che le connessioni tra gli utenti iChat possano funzionare correttamente tramite NAT (Network Address Translation)*.
5897-5898	UDP	(utilizzo non registrato)	–	xrdiags
5900	TCP	Virtual Network Computing (VNC) (utilizzo non registrato)	–	Apple Remote Desktop 2.0 o versioni successive (funzionalità Observe/Control) Condivisione schermo (Mac OS X v10.5 o versioni successive)
5988	TCP	WBEM HTTP	–	Apple Remote Desktop 2.x (http://www.dmtf.org/about/faq/wbem)
6970- 9999	UDP	–	–	QuickTime Streaming Server
7070	TCP	RTSP (utilizzo non registrato) Automatic Router Configuration Protocol (ARCP – utilizzo registrato)	–	QuickTime Streaming Server (RTSP)
7070	UDP	Alternativa RTSP	–	QuickTime Streaming Server
7777	TCP	Proxy di trasferimento file del server iChat (utilizzo non registrato)	–	–
8005	TCP	Chiusura Tomcat remota	–	–
8080	TCP	Porta alternativa per Apache	–	–
8085- 8087	TCP	Servizio Wiki	–	Mac OS X Server v10.5 e versioni successive
8088	TCP	Servizio Aggiornamento Software	–	Mac OS X v10.4 e versioni successive
8089	TCP	Regole email Web	–	Mac OS X Server v10.6 e versioni successive
8096	TCP	Reimpostazione password Web	–	Mac OS X Server v10.6.3 e versioni successive
8170	TCP	HTTPS (servizio/sito Web)	–	Podcast Capture/podcast CLI
8175	TCP	Pcast Tunnel	–	pcastagentd (per il controllo delle operazioni)
8000- 8999	TCP	–	–	Servizio Web, stream iTunes Radio
8821	TCP	Stored (server di archiviazione per la comunicazione con il server)	–	Final Cut Server
8891	TCP	ldsd (trasferimento dati)	–	Final Cut Server
9006, 8080, 8443	–	Porte HTTP e HTTPS per Tomcat Standalone e JBOSS (J2EE)		– –
11211	–	memcached (utilizzo non registrato)		Server iCal
16080	TCP	–	–	Servizio Web con cache di prestazioni
16384 16403	UDP	Real-Time Transport Protocol (RTP), Real-Time Control Protocol (RTCP)	–	iChat AV (Audio RTP, RTCP; Video RTP, RTCP)
24000 24999	TCP	–	–	Servizio Web con cache di prestazioni
42000 42999	TCP	–	–	Stream iTunes Radio
50003	–	Servizio server FileMaker	–	–
50006	–	Servizio di supporto FileMaker	–	–

*Il servizio SNATMAP comunica semplicemente ai client l'indirizzo Internet collegato ad esso. Questo servizio viene eseguito su un server Apple, ma non invia informazioni personali ad Apple. Il servizio viene contattato quando si utilizzano alcune funzionalità AV di iChat. Bloccare questo servizio può causare problemi nelle connessioni AV iChat con gli host su network che utilizzano NAT.

PROGRAMMARE CON MOZILLA

PROGRAMMING

Il motore di rendering made in Mozilla, lo stesso di Firefox, grazie a XPFE (Mozilla's cross-platform Front End) può diventare un interessante ambiente di sviluppo.

Mozilla dispone di un motore (rendering engine) chiamato Gecko, che insieme a XPCOM/XPConnect e XPFE permette di creare il browser riducendone i tempi di sviluppo, solo una parte del suo codice è diversa a seconda della piattaforma su cui dovrà girare. Questo avviene grazie a XPFE (acronimo di Mozilla's cross-platform Front End). Mozilla è ormai diventato ben più di un browser, è un framework per lo sviluppo di applicazioni cross-platform. Un computer in grado di eseguire Mozilla potrà eseguire qualunque applicazione di tipo Mozilla, indipendentemente dal sistema operativo usato.

Per fare un esempio, caricate il browser e aprite l'URL chrome://navigator/content, vedrete lo stesso browser eseguito all'interno di se stesso, come se fosse una normale pagina web.

MOZILLA JOBS...

Un'applicazione Mozilla è scritta facendo uso di diverse componenti:
XUL (acronimo che corrisponde a XML-based User Interface Language), un linguaggio cross-platform in grado di definire un'interfaccia utente per un'applicazione.

CSS (Cascading Style Sheets), permette di definire l'aspetto dell'applicazione.
Javascript per scrivere il codice del programma.
RDF (Resource Description Framework) per trasmettere informazioni e/o contenere dei dati.
XBL (eXtensible Binding Language), definisce widgets, parti riutilizzabili composte da codice XUL e Javascript.
XUL Templates, per importare dati nell'applicazione per mezzo di XUL e RDF.
DTD (Document Type Definition) permette di internazionalizzare l'applicazione facilitandone la traduzione in diverse lingue.
XPCOM/XPConnect (Cross Platform Component Object Model) permette al codice javascript di accedere al codice delle librerie esterne generalmente scritte in C (una tecnologia simile a COM di Microsoft).
XPInstall (Cross Platform Install) per installare package dell'applicazione su qualunque piattaforma.

Un'applicazione caricata dal browser ha generalmente delle limitazioni (principalmente a causa di motivi di sicurezza), per poterla eseguire al di fuori di esso si deve organizzarla come package e registrarla nel chrome registry. Abbiamo visto prima l'URL chrome://navigator/content, un URL che inizia con chrome:// permette di riferirsi ai packages installati nel sistema chrome di Mozilla.
Esaminando la directory di Mozilla possiamo trovare la subdirectory chrome, qui ci sono tutti i packages forniti con Mozilla. Un package consiste in un gruppo di directories e files con cui viene creata l'applicazione. Per maggior precisione si hanno tre gruppi di files (generalmente ognuno nella propria directory): content, locale e skin. L'applicazione può risiedere anche in un file archivio di tipo JAR (un file compresso con Zip dall'estensione .jar) ma la suddivisione in sub-directories è generalmente la stessa. Per complicare le cose un'applicazione può essere costituita anche da più packages, e un package può riferirsi a più applicazioni, per esempio, il browser è suddiviso tra comm.jar (content), en-US.jar (locale), modern.jar e classic.jar (skin, una per il theme Classic e l'altra per quello Modern). Normalmente un'applicazione è costituita da un solo package, suddiviso nei suoi tre tipi di componenti, ognuno nella sua directory (mettere tutti i files in una sola directory preclude la possibilità di usare skins e lingue diverse per l'applicazione).

Content
Qui risiedono i files XUL, le definizioni di ogni interfaccia utente dell'applicazione. Si possono avere più windows, ciascuna definita nel suo file (estensione .xul), ma quello che contiene la window principale deve avere come nome lo stesso del package in cui è contenuta. Insieme agli XUL possiamo avere anche files XBL che definiscono i widgets (estensione .xml) e i files che contengono il codice javascript (estensione .js).
Locale
È dove vengono collocati i files che contengono i testi che devono essere visualizzati dall'applicazione. Ogni testo visualizzato dovrebbe essere definito in uno di questi files. Vengono usati files DTD (estensione .dtd) contenenti le Entities da usare nei files XUL, files Properties (estensione .properties) contenenti le stringhe utilizzabili da javascript, files RDF (estensione .rdf) ed eventuali files HTML o XHTML. Potrebbero esserci anche dei files immagini, se questi sono diversi al variare della lingua.
Skin
Qui si hanno i files che definiscono l'aspetto dell'applicazione, quindi i files CSS e le immagini usate dal programma. Anche qui potrebbero esserci dei files di tipo XBL.

Per fare un esempio realizziamo un programma, helloworld. Costruiamo un package creando all'interno della directory chrome una subdirectory con il nome del nostro package, helloworld, e le sue tre subdirectories: content, locale e skin. Definite le subdirectories è necessario far conoscere la loro esistenza a Mozilla tramite dei files manifest. Un file manifest, in formato RDF e di nome contents.rdf, descrive cosa contiene la directory in cui si trova, c'è di solito uno di questi files per ogni suddivisione del package da noi creata.
Mozilla all'esecuzione legge il file installed-chrome.txt per sapere quali sono i packages da installare e, per mezzo dei files contents.rdf in essi definiti, li registra nel suo chrome registry che risiede in chrome.rdf. Installed-chrome.txt è un semplice file di testo che elenca i vari content, skin e locale che devono essere registrati nel chrome system, uno per riga. Per installare un package dobbiamo solo elencarvi quali questi siano per la nostra applicazione ed eseguire Mozilla. Una riga del file è composta da alcuni campi separati da una virgola, ad esempio:
content,install,url,resource:/chrome/helloworld/content/

Tipo: contiene content, skin oppure locale definisce il tipo di chrome che stiamo installando.
Tipo di installazione: contiene install (tutti i profili) o profile (singolo profilo), definisce come deve essere installato.
Tipo di URL: contiene url o path, nel primo caso è usato un URL per specificare dove si trova il package, nel secondo viene usato un file path.
URL: contiene l'url (o il path) del package, e per essere precisi la directory con il file contents.rdf del package. La stringa deve terminare con il carattere "/" essendo una directory.

Un URL resource (resource:/) è di un tipo particolare per il quale la sua radice è la directory in cui è installato Mozilla, inoltre ha un solo carattere "/" dopo la stringa resource.
L'aggiunta delle righe riguardanti la nostra applicazione al file può essere fatto manualmente o tramite uno script di installazione (noi useremo il primo metodo).

Quello che segue è un tipico contents.rdf per la directory content riferito a helloworld:

```
<?xml version="1.0"?>
<RDF:RDF xmlns:RDF="http://www.
w3.org/1999/02/22-rdf-syntax-ns#"
         xmlns:chrome="http://www.mozilla.
org/rdf/chrome#">
  <RDF:Seq about="urn:mozilla:package:root">
```

```
    <RDF:li resource="urn:mozilla:package:hell
oworld"/>
  </RDF:Seq>
  <RDF:Description about="urn:mozilla:package
:helloworld"
        chrome:displayName="Hello
World!" chrome:author="L'autore"
chrome:description="Esempio"
        chrome:name="helloworld"
chrome:localeVersion="1.2"
chrome:skinVersion="1.2">
  </RDF:Description>
</RDF:RDF>
```

Il file è di tipo XML, abbiamo quindi la dichiarazione XML come prima riga del file, seguita, come attributi del tag <RDF>, da quelle dei namespaces, uno per RDF e l'altro per il sistema chrome. Si ha poi la definizione di quale sarà il package descritto dal file manifest con l'attribuzione della resource relativa a helloworld (<RDF:li resource="urn:mozilla:package:helloworld"/>) alla sequenza dei packages di Mozilla (<RDF:Seq about="urn:mozilla:package:root">). Vengono poi fornite delle informazioni sul package tramite <RDF:Description about="urn:mozilla:package:helloworld"…>. Il valore dell'attributo resource di <RDF:li> e about di <RDF:Description> deve essere lo stesso in modo che il secondo si riferisca al primo.

In Mozilla sono generalmente definiti due themes, Classic e Modern, per la Skin della nostra applicazione possiamo riferirci ad uno di essi, ad esempio a Classic. Per facilitare l'aggiunta di altre skin separiamo la nostra skin in una sub-directory della directoty skin di nome classic. Il file contents.rdf è definito in questo modo per la directory classic:

```
<?xml version="1.0"?>
<RDF:RDF xmlns:RDF="http://www.
w3.org/1999/02/22-rdf-syntax-ns#"
         xmlns:chrome="http://www.mozilla.
org/rdf/chrome#">
<RDF:Seq about="urn:mozilla:skin:root">
 <RDF:li resource="urn:mozilla:skin:classic/
1.0"/>
</RDF:Seq>
<RDF:Description about="urn:mozilla:skin:clas
sic/1.0">
 <chrome:packages>
  <RDF:Seq about="urn:mozilla:skin:classic/1.
0:packages">
   <RDF:li resource="urn:mozilla:skin:classic
/1.0:helloworld"/>
  </RDF:Seq>
 </chrome:packages>
</RDF:Description>
<RDF:Description about="urn:mozi
lla:skin:classic/1.0:helloworld"
chrome:skinVersion="1.2"/>
</RDF:RDF>
```

Viene per prima cosa specificato che la skin/theme a cui ci stiamo aggiungendo è la classic tramite i tags <RDF:Seq> e <RDF:li> iniziali. Per mezzo di <chrome:packages> viene definito che la skin dovrà essere usata per il package helloworld ed infine viene assegnata una versione alla nostra skin.

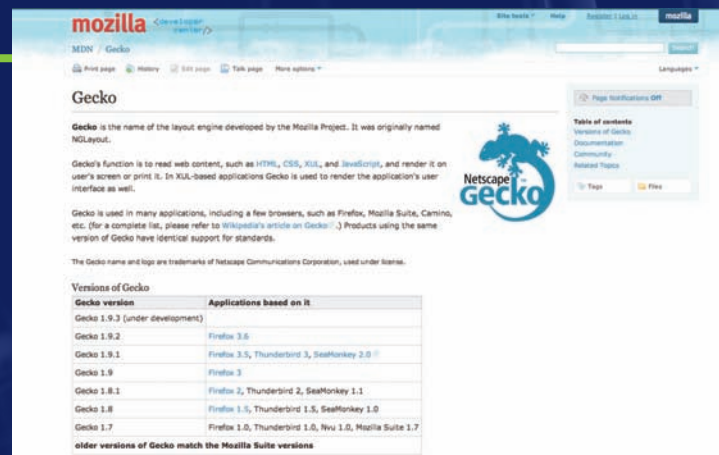
Questo è il file CSS (helloworld.css) per la skin Classic:

```
@import url(chrome://global/skin/);
.windowmain{ background-color: black; di-
splay: block; width: auto; height: auto; }
.buttons{ background-color: white; color:
blue; }
.buttons:hover{ background-color: lightblue;
color: black; }
```

La prima riga, @import url(chrome://global/skin/);, ci permette di importare nel nostro file CSS la skin global (default per gli elementi XUL) del theme selezionato. Le righe seguenti definiscono le classi da noi usate per gli elementi di cui vogliamo modificare lo stile.

Nell'installazione di Mozilla è già presente un package per una lingua, in genere l'inglese, possiamo quindi definire il file contents.rdf per la directory locale di helloworld in modo che estenda la lingua inglese, en-US, per la nostra applicazione:

```
<?xml version="1.0"?>
<RDF:RDF xmlns:RDF="http://www.
w3.org/1999/02/22-rdf-syntax-ns#"
         xmlns:chrome="http://www.mozilla.
org/rdf/chrome#">
<RDF:Seq about="urn:mozilla:locale:root">
 <RDF:li resource="urn:mozilla:locale:en-
US"/>
</RDF:Seq >
<RDF:Description
about="urn:mozilla:locale:en-US"
      chrome:displayName="English(US)"
chrome:author="L'autore" chrome:name="en-US"
 <chrome:packages>
  <RDF:Seq about="urn:mozilla:locale:en-
US:packages">
   <RDF:li resource="urn:mozilla:locale:en-
US:helloworld"/>
  </RDF:Seq>
 </chrome:packages>
</RDF:Description>
 <RDF:Description
about="urn:mozilla:locale:en-US:helloworld"
chrome:localeVersion="1.2"/>
</RDF:RDF>
```

Come potete vedere è molto simile a quello usato per Skin, e definisce che si vuole aggiungere qualcosa al language pack inglese tramite i tags <RDF:Seq> e <RDF:li> iniziali e che quello che si vuole aggiungere è la risorsa locale di helloworld (<chrome:packages>…</chrome:packages>).

Se suddividiamo la nostra directory locale in subdirectories, una per ogni lingua, possiamo rendere più semplice l'operazione di aggiungervi un'altra lingua, creiamo quindi una subdirectory en-US della locale ed in essa, assieme a contents.rdf, mettiamo il file helloworld.dtd contenente:

```
<!ENTITY buttonhello.lbl "Hello">
<!ENTITY buttonclose.lbl "Close">
```

Aggiungiamo in questa directory anche il file strings.properties con il testo da usare da javascript (il formato è: il nome della stringa seguito dal segno "=" ed infine il testo della stringa):

```
message=Hello World!
```

Questo è infine il file helloworld.xul presente nella directory content:

```
<?xml version="1.0"?>
<?xml-stylesheet href="chrome:helloworld/
skin/helloworld.css" type="text/css"?>
<!DOCTYPE window SYSTEM "chrome://helloworld/
locale/helloworld.dtd" >
<window xmlns="http://www.mozilla.org/
keymaster/gatekeeper/there.is.only.xul"
class="windowmain">
 <script type="application/x-javascript"
src="chrome://helloworld/content/helloworld.
js" />
 <stringbundle id="strings" src="chrome://
helloworld/locale/strings.properties" />
 <box>
  <button class="buttons"
label="&buttonhello.lbl;"
oncommand="hello();" />
  <button class="buttons"
label="&buttonclose.lbl;"
oncommand="closeApp();" />
 </box>
</window>
```

XUL E XML

La prima riga di un file XUL deve contenere sempre la dichiarazione XML, ad essa segue la definizione del CSS da utilizzare (<?xml-stylesheet...?>) e quella che indica dove trovare le entities da utilizzare per il locale selezionato (<!DOCTYPE ...>).
Subito dopo incontriamo l'elemento window, uno degli elementi usati per racchiudere l'applicazione, il contenitore principale, tutti gli altri elementi sono al suo interno e sono suoi children (figli). Come attributo di questo elemento c'è la definizione del namespace, questo serve a dichiarare quali sono gli elementi validi che possono essere inclusi nel file XUL.
Il codice javascript associato ai buttons è incluso nello XUL con il tag <script .../> e l'elemento <stringbundle> che lo segue serve per accedere al file .properties da javascript per i testi (il suo attributo src è l'URL al file strings.properties presente in locale).

All'interno dell'elemento window troviamo un elemento box, che serve da contenitore per i due elementi buttons le cui labels fanno riferimento alle due entities &buttonhello.lbl; e &buttonclose.lbl;definite nel file DTD.

Il file helloworld.js è composto semplicemente da due funzioni, una per ciascuno dei buttons:

```
function hello(){
 var mystringbundle=document.
getElementById("strings");
 var message=mystringbundle.
getString("message");
 alert(message);
}
function closeApp(){
 window.close();
}
```

L'unica a richiedere spiegazioni è la funzione hello, l'elemento <stringbundle> presente nel file XUL ci permette di leggere i testi delle stringhe contenute nel file .properties. Per prima cosa dobbiamo accedere a questo elemento (questo avviene usando il metodo getElementById(IdElemento) dell'elemento document) ottenutolo, nella variabile mystringbundle, possiamo usarlo per avere il testo della stringa di nome message con il suo metodo getString(nomedellastringa) e visualizzare il testo con la funzione alert.
Per completare l'applicazione non rimane che aggiungere al file installed-chrome.txt le righe riguardanti helloworld:

```
content,install,url,resource:/chrome/hel-
loworld/content/
locale,install,url,resource:/chrome/hel-
loworld/locale/en-US/
skin,install,url,resource:/chrome/helloworld/
skin/classic/
```

Per eseguire un'applicazione senza passare dal browser si deve fornirne il suo nome a Mozilla come parametro per mezzo di un URL chrome: per eseguire helloworld la linea di comando da usare è mozilla -chrome chrome://helloworld/content, ove -chrome segnalata a Mozilla che seguirà un URL di tipo chrome da caricare direttamente.

INDIRIZZI UTILI

https://developer.mozilla.org/En/Toolkit_API
https://developer.mozilla.org/en/Gecko

RETI/MEDIO

Andrea Draghetti
info@oversecurity.net

Il Reverse Engineering di FastWeb

RETI

Come ricavare l'algoritmo di assegnazione della chiave WPA e WEP di un Access Point FastWeb.

Il Reverse Engineering è la migliore tecnica per analizzare nel dettaglio il funzionamento di un qualsiasi codice del quale non si conosca il sorgente, Ben Affleck nel famoso film Paycheck di John Woo ci illustra tale processo copiando un prodotto elettronico di un'altra azienda concorrente.
In questo articolo applicheremo il Reverse Engineering agli Access Point FastWeb per analizzare e ricavare l'algoritmo di assegnazione della chiave WPA e WEP.

Access Point

Accendendo l'Access Point il primo dato più evidente è SSID (il nome della rete Wireless), così formato: "Fastweb-Y-xxxxxxxxxxxx" dove Y può assumere il valore 1 o 2 e le x rispecchiano il MAC Address della scheda wireless interna. Dalle prime 3 coppie del MAC è quindi possibile capire il produttore dell'Access Point. Noi analizzeremo un Access Point Pirelli identificabile dalle seguenti prime tre coppie di MAC Address: 00:08:27, 00:13:C8, 00:17:C2, 00:19:3E, 00:1C:A2, 00:1D:8B, 00:22:33, 00:23:8E, 00:25:53.

Analisi dell'algoritmo

In sintesi questi sono i passi svolti dall'algoritmo per ricavare la WPA o WEP predefinita partendo dal SSID:

1. Estrae una sequenza di 6 byte dal SSID.
2. Inizializza i vettori MD5 (MD5Init).
3. Inserisce i 6 byte del SSID nella sequenza di cui calcola l'hash MD5 (MD5Update).
4. Ricalcola l'hash MD5 (dell'hash precedente) utilizzando una sequenza di 20 byte predefinita (MD5Update).
5. Finalizza l'hash MD5 (MD5Finish).
6. Dall'hash finale crea una sequenza binaria ottenuta considerando i primi 4 byte più significatividell'hash.
7. Questa sequenza viene a sua volta suddivisa in 5 gruppi da 5 bit ciascuno. I bit in eccesso vengono scartati. Ed ogni gruppo di 5 bit viene riconvertito in esadecimale (*) riottenendo una sequenza di 5 byte.
8. Somma 0°—57 ad ogni byte il cui valore sia >= 0xA (**).
9. La concatenazione di queste rappresentazioni (con lettere minuscole) è la WPA o WEP di default.

(*) Una sequenza da 5 bit può assumere il valore compreso tra 0°—00 e 0°—1F.
(**) L'aggiunta della costante 0°—57 avviene poiché i caratteri tra 0xA e 0°—60 (estremi inclusi) non sono validi nello spazio chiavi considerato, per cui aggiungendo

0°—57 a 0xA si ottiene, appunto, ox61 (primo carattere ammesso dopo 0°—09).

I punti 2, 3 e 4 dell'algoritmo sono svolti dalla funzione cript_it; essa riceve in input una sequenza di 6 byte ottenuta dalla parte terminale del SSID raggruppando i byte in 6 gruppi da 2 cifre cadauno (00,12,34,56,78,90) e ne calcola MD5, algoritmo crittografico di hashing realizzato da Ronald Rivest nel 1991 e standardizzato con la RFC 1321.

Per migliorare l'algoritmo hanno aggiunto un salt (unk_100220D0), ovvero una sequenza speciale prefissata di 0°—14 (20) byte, da inserire nella sequenza alterando in modo originale la creazione dell'hash MD5.

Di seguito è riportato un estratto della funzione in questione (cript_it).

```
Cript_it
.text:00480FF8 la $t9, atomac
.text:00480FFC jalr $t9 ; atomac
.text:00481000 move $a0, $s0
.text:00481004 lw $gp, 0xA8+var_98($sp)
.text:00481008 move $s0, $v0
.text:0048100C addiu $a0, $sp, 0xA8+var_90
.text:00481010 beqz $s1, loc_48109C
.text:00481014 la $t9, MD5Init
.text:00481018 jalr $t9 ; MD5Init
.text:0048101C nop
.text:00481020 lw $gp, 0xA8+var_98($sp)
.text:00481024 move $a1, $s0
.text:00481028 addiu $a0, $sp, 0xA8+var_90
.text:0048102C la $t9, MD5Update
.text:00481030 jalr $t9 ; MD5Update
.text:00481034 li $a2, 6
.text:00481038 lw $gp, 0xA8+var_98($sp)
.text:0048103C addiu $a0, $sp, 0xA8+var_90
.text:00481040 li $a2, 0x14
.text:00481044 la $a1, 0x10020000
.text:00481048 la $t9, MD5Update
.text:0048104C jalr $t9 ; MD5Update
.text:00481050 addiu $a1, (unk_100220D0 - 0x10020000)
.text:00481054 lw $gp, 0xA8+var_98($sp)
.text:00481058 addiu $a0, $sp, 0xA8+var_20
.text:0048105C la $t9, MD5Final
.text:00481060 jalr $t9 ; MD5Final
```

Conoscendo il delay slot, è evidente che l'indirizzo della sequenza segreta è unk_100220D0. A tale indirizzo troviamo:

0x22,0x33,0x11,0x34,0x02,0x81,0xFA,0x22,0x11,0x41,0x68,0x11,0x12,0x01,0x05,0x22,0x71,0x42,0x10,0x66

ESEMPIO PRATICO

La nostra rete Fastweb ha un SSID così composto:

FASTWEB-1-00193EA1B2C3.

Prendiamo pertanto in considerazione i 6 byte: 00,19,3E,A1,B2,C3.
Si calcola l'hash MD5 di questi 6 byte secondo l'algoritmo sopracitato ottenendo:
a37d4267f1d177f44d352978-d95558a9.

Di questo hash si considerano i primi 4 byte nella rappresentazione binaria, ovvero 10100011 01111101 01000010 01100111. Prendiamo questa sequenza e creiamo cinque gruppi di 5 bit ciascuno, ottenendo: 10100 01101 11110 10100 00100, che rappresentati in esadecimale diventano 0°—14 0°—0D 0°—1E 0°—14 0°—04. La chiave WPA e WEP si ottiene da questa sequenza di byte confrontando ciascun byte con 0°—0A, se risulta essere maggiore viene aggiunto il valore hex 0°—57, ricavando così la chiave: 6b64756b04.

CONCLUSIONI

Appare evidente che legare univocamente la chiave SSID alla chiave WEP o WPA non è stata sicuramente la scelta più corretta, assegnare la chiave a informazioni interne dell'Access Point non deducibili da alcuna combinazione di MAC o ESSID sarebbe stata una scelta più accurata. Siamo pertanto a consigliarvi di cambiare la chiave WPA e WEP di default del proprio Access Point.

Miclen
miclen.developers@gmail.com

INSTALLARE android su Samsung Omnia

MOBILE

Breve guida per installare Android su Samsung Omnia.

Android, il nuovo sistema operativo mobile targato Google è disponibile da diversi mesi sui nuovi dispositivi mobile in commercio. La new entry presenta un bellissimo design intuitivo e rapido, il sistema è fluido e non presenta particolari bug. Sembra che la "famiglia Google" abbia sviluppato un buon sistema operativo M.

PORTABILITÀ

Il problema principale di Android è la portabilità, un fattore molto critico e importante per un sistema operativo mobile. Nonostante tutte le modifiche apportate da Google non si è arrivati ancora ad una release stabile per tutti i dispositivi. Su internet, all'indirizzo www.androidomnia.com è reperibile un progetto free da cui è possibile scaricare i file per effettuare il porting . Il progetto è sponsorizzato dalle donazioni degli utenti.

COMPATIBILITÀ CON OMNIA

Le modifiche apportate al nuovo sistema Android sono numerose e tuttora, come detto, non si è riusciti ancora a sviluppare una release stabile e funzionale del sistema Google , le funzionalità supportate sono diverse , ma la versione disponibile per il download non è ancora in grado di gestire Bluetooth, GPS, fotocamera , modalità sospensione e anche altre funzioni ugualmente importanti.
Si tratta du una "release ponte", dunque nei prossimi rilasci è lecito aspettarsi che queste funzionalità siano progressivamente implementate.

INSTALLAZIONE

Dopo avere effettuato una panoramica generale del nuovo sistema, è venuto il momento di passare alla pratica, ovvero all'installazione:

Su internet è disponibile un progetto free all'indirizzo www.androidomnia.com da cui è possibile scaricare i file per effettuare il porting di Androd su altri dispositivi mobili. Gli stessi file sono reperibili ll'indirizzo www.hackerjournal.it, nella sezione download.

- Copiare la cartella haret downlodabile dal sito www.hackerjournal.it (sezione download).
- Formattare la microsd presente nel cellulare con il filesystem ext3.

2.1 Per formattare la microsd bisogna utilizzare un partition editor presente di default nella distro ubuntu scaricabile da http://www.ubuntu-it.org/download.shtml.
2.2 Fare un backup di tutti i dati.
2.3 Avviare il sistema operativo appena scaricato.
2.4 Andare su system -> administrator -> partition editor.
2.5 Cancellare la partizione esistente e crearne una con filesystem ext3 (per Android bastano meno di 500 mb) e poi con lo spazio restante crearne una in fat32 (ps. La partizione ext3 non è visibile da Windows).
2.6 Per copiare i file nella nuova partizione ext3 dobbiamo aprire il terminale presente nella categoria applicazione e digitare:

```
sudo cp indirizzo file,
indirizzo destinazione
Esempio : sudo cp media/
data/android /media/disk.
```

Con questo comando è possibile copiare i file. Se il terminale restituisce qualche errore utilizzare il comando mv

- Copiare il contenuto della cartella andromania_rootfs (link in allegato) nella microsd
- il file default.txt contenuto in haret sostituendo mmcblk0p5 con mmcblk0p1
- Il nostro sistema è pronto per essere avviato :) , avviare haret passato in precedenza e cliccare su run
- Per selezionare la lingua italiana andare su Setting -> locale & text -> Select Locale

Il nuovo sistema Android presenta una piccola innovazione, è possibile installare nuove applicazioni automaticamente passando i file *.apk nella dir /system/app.

:: POSTA ::

VERSIONE PDF

Cari amici , ormai è da tanto tempo che vi seguo ma ultimamente ho molte difficoltà a "rintracciarvi". A marzo ho dovuto fare salti mortali per trovare la rivista... ed è ormai da inizio aprile 2010 che non riesco più a rintracciarvi in nessuna edicola della mia zona. Ho controllato e chiesto in tutte le edicole in zona nell'arco di 30 km ma nessuno riesce a ricevervi.
Ho chiesto ad alcuni miei negozianti di fiducia se riuscivano a rintracciarvi ma tutti hanno detto che ci sono dei problemi nelle consegne per le poche quantità prodotte.
Visto che non date la possibilità dell'abbonamento cartaceo perché non crearne uno per la consegna in pdf?
Sarei davvero contento di pagare per ricevervi sulla mia e-mail ogni 14 giorni in pdf!
Fatemi sapere come posso fare a "ritrovarvi".

Mandaglio Ferdinando

Secondo i dati che in genere si snocciolano durante le riunioni "per farsi belli" sembra che in Italia esistano circa 33.000 edicole censite a cui si sommano poi i punti vendita alternativi creati dopo la liberalizzazione (soprattutto i supermercati). Evidentemente coprire tutte le edicole non è semplice, occorrono tirature molto grandi, specie se si considera che alcune edicole, dove c'è più richiesta, ricevono più di una copia. Capita quindi che alcune edicole, dove non c'è molta richiesta, finiscano per essere escluse dalle logiche della distribuzione.
Comunque l'edicolante può cercare di contattare proprio il distributore, che magari lo rifornisce anche di altre riviste, per cercare di farsi mandare almeno una copia di HJ.
Ma questa è solo una disquisizione tecnica. Quello che invece abbiamo trovato interessante della tua mail è l'idea dell'abbonamento ad una versione pdf da inoltrare via mail o da scaricare direttamente da una sezione dedicata del sito.
In effetti sono davvero molti quelli che ci chiedono la possibilità di abbonarsi al giornale cartaceo, possibilità purtroppo esclusa, e questa soluzione potrebbe essere un giusto compromesso.
Vi piace l'idea? Voi vi abbonereste? Fateci sapere la vostra opinione perché l'abbonamento alla versione digitale in .pdf potrebbe essere una via percorribile.

SOFTWARE FREE E OPEN SOURCE DIFFERENZE OGGETTIVE E FILOSOFIA SOSTANZIALE

Scrivo in risposta all'articolo riguardante Richard Stallman pubblicato sul penultimo numero.
Questa lettera non vuole esser provocatoria ma, anzi, è una richiesta personale di chiarimento che spero possa trovare spazio sulla rivista e aiuti quanti abbiano i miei medesimi dubbi o altri ad essi correlati.
Perdonatemi se ho interpretato male le vostre affermazioni o se il tono da voi utilizzato mi è sembrato acceso ma proprio non capisco se il vostro vuol essere un "attacco" alla persona sopra citata, all'ideale del free software, della FSF o di GNU oppure nulla di tutto questo.
Prima di tutto non capisco la vostra posizione, sì, è banale la cosa, ritengo di parlare con degli Hacker, nel senso più alto del termine, lo dico con stima, a maggior ragione dopo aver partecipato alla presentazione della facoltà di Ingegneria Informatica al Politecnico di Milano (27-03-2010) durante la quale è stato più volte impropriamente utilizzato il termine "Hacker" per indicare la categoria più infima/subdola dei "Lamer" (oltre al fatto che sono stati portati esempi di tecnologia un po' ridicoli quali la lavatrice o l'iPod... e i sistemi embedded sono stati appena accennati...).
Negli anni che ho seguito la rivista ho imparato che alla base della figura dell'hacker ci debba essere una spiccata curiosità; ciò è fondamentale affinché la conoscenza personale si possa approfondire e venga a sua volta condivisa con quanti ci stanno attorno (ancora i discorsi si mescolano, questa idea è dell'hacking? Dell'open source? Del free software? O di tutti un po'?).
Comunque, tornando all'oggetto della questione: voi da che parte state? Siete fra i "puristi" che ben distinguono Linux e GNU? Se sì, cosa li differenzia "nell'ideale"? Cosa cambia fra free software e open source?
A me pare che l'uno sia parte integrante dell'altro, insomma, anche qua ci sarebbe da discutere...,
perché un software sia libero dev'essere necessariamente open? Quindi, in definitiva, il promuovere un qualcosa che si può modificare liberamente, che si può sviluppare, che può essere perfino venduto (alla luce del fatto che chi anche lo comprasse, ne avrebbe il sorgente e lo avrebbe potuto scaricare liberamente in altra sede...) per quanto sia "libero", è secondo voi sbagliato? Differisce dall'idea di "open"?
Da quello che ho potuto comprendere dalla vostra pubblicazione (che per ovvie ragioni editoriali non può essere una mera trasposizione dell'intero discorso tenutosi alla conferenza) ritengo che Stallman porti in ambito software l'idea molto ampia e con mille sfaccettature di libertà.
Perché quest'idea secondo voi non può funzionare?
Concludendo, voglio motivare ulteriormente la decisione di scrivere questa lettera!
Ritengo che abbiate espresso velatamente un'idea e per creare un confronto costruttivo, per avere uno scambio di idee, vorrei che la esplicitaste.
Vi invito pertanto a parlare liberamente, in prima persona.

Marco

:: POSTA ::

Open source e software libero rappresentano due facce diverse di una medaglia che per certi versi è la stessa. Per molti Linux è un po' l'emblema del software libero. Linux fa parte infatti del progetto GNU (acronimo ricorsivo : Gnu's Not Unix) supportato dalla Free Software Foundation.
Il progetto GNU è una "creatura" di Richard Stallman e ha come obiettivo la creazione e diffusione proprio di software libero.
Secondo i criteri stessi della Free Software Foundation è definito software libero quel software che garantisce all'utente:

- La libertà di eseguire il programma, per qualsiasi scopo.
- La libertà di studiare come funziona il programma e adattarlo alle proprie necessità (quindi il sorgente deve essere pubblico).
- La Libertà di ridistribuire copie in modo da aiutare il prossimo.
- La Libertà di migliorare il programma e distribuirne pubblicamente i miglioramenti, in modo tale che tutta la comunità ne tragga beneficio.

Fin qui non fa una piega: perfetto, il cerchio parrebbe chiuso.
Eppure Linux è anche un sistema Open Source, ovvero un programma aperto che consente a chiunque di vedere i codici sorgente e di modificarli secondo le proprie esigenze.
Quindi verrebbe da dire che Open Source e Software Libero sono la stessa cosa... Invece esiste una sottile differenza, perché l'Open Source ha come scopo prioritario quello di garantire l'accesso al cuore programma ma non si preoccupa che i programmi e le informazioni siano liberamente disponibili, mentre il software libero deve conservare le quattro libertà statutarie.
Da sottolineare che il software libero non deve essere, come del resto l'open source, necessariamente gratuito, nulla vieta, infatti, a qualcuno di confezionare un software libero, aggiungerci dei manuali e un servizio di supporto e farsi pagare il tutto. Anzi, questa é una delle libertà che la FSF difende.
Ma quel software libero deve mantenere le quattro libertà fondamentali dell'utente.
A bene vedere si tratta di differenze formali più che sostanziali, ma sono differenze che gli stessi fautori del software libero e dell'open source difendono e rimarcano in ogni occasione. Quindi se provate a parlare di open source con Stallman probabilmente verrete ripresi come lo sventurato giornalista di cui abbiamo parlato nell'articolo. Sono filosofie a confronto, forse anche un po' radicali, ma devono essere rispettate come tali e noi non possiamo certo cercare di sovvertirle.
Per quanto riguarda l'idea di libertà intesa in senso lato, quella che tutto sommato viene fuori dai discorsi di Richard Stallman, a noi piace parecchio.
Se nell'articolo traspariva un'opinione diversa non era nostra intenzione, non rispecchia quello che pensiamo. Semmai il problema è che si tratta di un'idea filosofica meravigliosa ma di difficile attuazione nella società attuale. Occorre che i tempi maturino ancora un po' e forse la meravigliosa utopia di RS diverrà una concreta realtà come tutti noi speriamo.

APPROFONDIMENTI

Egregi signori,mi chiamo Yuri e scrivo dalla provincia della Spezia.
Ho 40 anni e sono veramente un profano col pc,nonostante ciò leggo regolarmente la vostra rivista (la compra mio figlio) anche, se ad essere sinceri, non sono all'altezza di capirci molto.
Perché vi scrivo?
Spiego: tramite la scuola di mio figlio, alcuni giorni fa, ho ricevuto visita di un "rappresentante" di una famosa casa editrice italiana che, a dire suo, mi proponeva un "sistema" per impedire al figliolo di navigare su siti poco indicati per un tredicenne.
Siccome sono spesso fuori per lavoro, mi sono fatto "fregare" e l'ho acquistato, installato e reso operativo.
Ho lasciato un post-it (più consono alla mia età) al figlio dicendo che, se riusciva a "bucare" il sistema acquistato, gli avrei comprato la chitarra nuova...
Quando ho riacceso il monitor la sera, era pieno di immagini di nudo... non solo, è anche riuscito (il figliolo) a spegnerlo senza sapere la password da me impostata.
L'indomani, ovviamente, ho esercitato il diritto di recesso e acquistato la chitarra nuova.
Mi consigliate, gentilmente, qualche lettura (oltre la vostra naturalmente) per cercare di capirci un pochino almeno di informatica e, col tempo, cercare di capire quello che fa il "giovane" e, se riesco, evitargli brutte esperienze.

Yuri

Ci verrebbe da dire che se tuo figlio ha bucato il sistema di sicurezza proposto dalla ditta, allora la rivista funziona...
A parte gli scherzi più che suggerirti una lettura (di libri ce ne sono davvero tanti, basta che vai in una grande libreria) ti suggeriamo di iscriverti al nostro forum su www.hackerjournal.it, se apri un post con le tue domande siamo sicuri che riceverai molti ottimi consigli.
Il forum è variegato come frequentazioni, ma, il livello è davvero alto e gli esperti sono davvero molti.
Poi, leggendo qua e là tra i vari post, siamo sicuri troverai anche argomenti piuttosto interessanti da approfondire...

Giovanni Federico - giovanni.federico@isek.it
Fabio `BlackLight` Manganiello - blacklight86@gmail.com

PARTE III

CORSO DI PROGRAMMAZIONE IN C

LINGUAGGI Siamo giunti alla terza parte del Corso di Programmazione ormai capaci di realizzare semplici applicativi utilizzando tutto quanto descritto nelle prime due parti. Giunge pertanto il momento di scoprire, come anticipato, alcune nozioni un attimino più "avanzate" che ci permetteranno di espandere le nostre possibilità implementative.

Oggetto di questa trattazione saranno quindi gli array (o vettori) mono/multidimensionali, gli algoritmi di ricerca lineare e dicotomica e gli algoritmi di ordinamento.
Come sempre, trovate tutti gli allegati e gli approfondimenti sul nostro sito web (www.hackerjournal.it).
Vi segnaliamo inoltre l'apertura di un forum dedicato esclusivamente al Corso di Programmazione che trovate all'indirizzo "www.hackerjournal.it/corsoc.htm": sicuramente un buon modo per confrontarsi con l'intera community offrendo spunti e suggerimenti di qualsiasi tipo.

VETTORI MONODIMENSIONALI

I vettori, o array, sono il tipo di struttura dati (Definizione 2 - HJ 200) più elementare gestibile in informatica, e presentano molte similitudini con i "cugini" trattati in algebra lineare.
Finora, fondamentalmente, abbiamo analizzato unicamente grandezze di tipo scalare , ovvero variabili (Definizione 5 - HJ 200) a sé stanti identificate da un nome e da un valore unico (carattere, numero intero, reale) contenuto al loro interno.
In informatica molto spesso si ha però a che fare con collezioni di dati, ovvero oggetti contenenti al loro interno più elementi, dello stesso tipo (Definizione 1 - HJ 200) o di tipi eterogenei.

Diamo pertanto la seguente:

DEFINIZIONE 20

Definiamo e denotiamo array o vettore un dato strutturato costituito da un insieme finito di valori dello stesso tipo identificato da un nome che individua collettivamente i predetti.
Ogni elemento occupa una ben determinata posizione in memoria.

Si pensi a un vettore come a una cassettiera ordinata di un archivio. Ogni cassetto è identificato da un numero, o indice, che identifica univocamente la sua posizione all'interno della "struttura", ed ha un contenuto.
Per accedere a un determinato elemento della cassettiera basta conoscere il suo indice ed il "cassetto" associato si apre. Un vettore in C, a differenza di altri linguaggi scarsamente o non tipizzati come Perl o Python, contiene solo elementi dello stesso tipo (si parla quindi di vettori di interi, di caratteri, di numeri reali, di stringhe, di tipi di dati strutturati ecc. ed ovviamente non è possibile inserire un tipo di dato strutturato all'interno di un vettore di interi, a meno che non si facciano opportune operazioni di cast - vedi richiamo teorico 4).

RICHIAMO TEORICO 4

TYPE CASTING.
Definiamo e denotiamo come operazione di type casting quella capace di modificare il tipo riferito da una variabile in un altro. In C l'operazione è effettuabile utilizzando l'operatore "()" come illustrato di seguito:

```
...
char sessantacinque = 'A';
int numero;

/*          Assegniamo alla variabile "nu-
mero" (intero) 65
 *          (ASCII code per il carattere 'A',
risultato
 */         del cast effettuato):

numero = (int) sessantacinque;
```

La dichiarazione di un vettore in C è molto semplice. Basta infatti dichiarare il tipo di dato, il nome del vettore e, fra parentesi quadre, il numero di elementi contenuti al suo interno:

```
int miovettore[10];
```

Questa scrittura dichiarerà un vettore di interi chiamato miovettore e contenente dieci elementi consentendoci di offrire la seguente:

> **DEFINIZIONE 21**
> DICHIARAZIONE DI UN ARRAY MONODIMENSIONALE.
>
> Un array (vettore) monodimensionale in C si dichiara mediante la seguente forma:
> <tipo> <nome>[<elementi>]; .

Bisogna stare attenti alla numerazione degli indici. Il fatto che il vettore appena dichiarato contenga dieci elementi vuol dire che i suoi elementi hanno indici che vanno da 0 a 9, non da 1 a 10.
Anche l'accesso agli elementi del vettore appena dichiarato è estremamente semplice. Se volessimo, ad esempio, copiare un valore nel primo elemento del vettore, basterebbe utilizzare una scrittura del tipo:

```
miovettore[0] = 1;
```

Se invece desideriamo riempire tutto il vettore con valori inseriti dall'utente, utilizzeremo un ciclo for (Definizione 12 - HJ 201):

```
int i;
int miovettore[10];

for (i=0; i < 10; i++) {
        fprintf (stdout, "Elemento n.%d:¬
", i+1);
        scanf ("%d", &miovettore[i]);
}
```

In modo del tutto simile, per stampare a video gli elementi contenuti all'interno del vettore:

```
for (i=0; i < 10; i++)
        fprintf (stdout, "L'elemento ¬
n.%d vale %d\n", i+1, miovettore[i]);
```

Si noti l'uso della variabile i, chiamata variabile indice, che spaziando sull'intervallo [0...9] cicla su tutti gli elementi del vettore.

È un po` come scorrere il dito sulla cassettiera di prima, dal primo all'ultimo elemento ed aprire tutti i cassetti per esaminarne il contenuto.

Un array può anche essere dichiarato in modo statico, ovvero specificandone il contenuto al momento della dichiarazione.

```
int miovettore[] = { 1,1,2,3,5,8,13,21 };
```

Inoltre, buona abitudine è quella di specificare, se possibile, la dimensione del vettore come costante (Definizione 6- HJ 200) o macro.
A differenza di linguaggi ad oggetti (OOP) come C++ e Java, infatti, in C un vettore è visto come una zona di memoria contenente dati fra loro adiacenti, non come un oggetto vero e proprio contenente al suo interno informazioni quali la dimensione e il tipo, o metodi come la ricerca e l'ordinamento.
Se nel nostro programma, ad esempio, volessimo gestire le informazioni anagrafiche di 200 utenti creando diversi vettori (uno per memorizzare i codici fiscali, uno per memorizzare nome e cognome, uno per l'età, e così via), questi avrebbero tutti la stessa dimensione, pari al numero di utenti da gestire.
Se un giorno il numero di utenti dovesse passare da 200 a 300, sarà necessario cambiare la capienza di tutti i vettori, magari dichiarati in momenti diversi, e dei valori di "arrivo" nei cicli for.
Se invece dichiariamo la dimensione come un parametro fisso, allora, ovviamente, basterà cambiare quel parametro, ed, automaticamente, tutta la logica verrà modificata per gestire la nuova dimensione.

```
#define    DIMENSIONE        10
...
int i;
int miovettore[DIMENSIONE];

for (i=0; i < DIMENSIONE; i++)

        /* Istruzioni */
```

Un buon esercizio è quello di calcolare la media aritmetica di n numeri forniti in input dall'utente utilizzando gli array. La media aritmetica è definita come la somma di tutti i valori diviso il numero degli stessi, da cui:

```
#include <stdio.h>
#define    MAXSIZE          10

int main() {
        int i, N;
        int numeri[MAXSIZE];
        float media = 0.0;

        do {
                fprintf (stdout, "Inserisci
il numero di valori di cui "
                        "vuoi calcola-
re la media (max. %d)\n",
                        MAXSIZE);
                scanf ("%d", &N);
        } while (N < 0 || N > MAXSIZE);

        for (i=0; i < N; i++) {
                fprintf (stdout, "Ele ¬
mento n.%d: ", i+1);
                scanf ("%d", ¬
&numeri[i]);
                media += (float) ¬
numeri[i];
        }

        media = media/N;
        fprintf (stdout, "Media dei %d ¬
valori inseriti: %f\n", N, media);
        return 0;
}
```

Una ulteriore applicazione esemplificativa potrebbe essere quella per il calcolo del prodotto scalare che prenda in input dall'utente due vettori, v1 e v2 (ricordandoci che il prodotto scalare tra due vettori si definisce come la quantità v1[0] * v2[0] + v1[1] * v2[1] + v1[2] * v2[2] + ...):

```
#include <stdio.h>
#define    MAXSIZE          10

int main() {
        int i, N;
        float v1[MAXSIZE], v2[MAXSIZE];
        float prod = 1.0;

        do {
                fprintf (stdout, "Inserisci
il numero di valori contenuti "
                        "nei vettori
(max. %d)\n",
                        MAXSIZE);
                scanf ("%d", &N);
        } while (N < 0 || N > MAXSIZE);

        for (i=0; i < N; i++) {
                fprintf (stdout, "Ele ¬
mento v1[%d]: ", i+1);
```

```
            scanf ("%f", &v1[i]);

            fprintf (stdout, ¬
"Elemento v2[%d]: ", i+1);
            scanf ("%f", &v2[i]);
      }

      for (i=0; i < N; i++)
            prod += (v1[i] * v2[i]);

      fprintf (stdout, "Prodotto scalare
dei due vettori: %f\n", prod);
      return 0;
}
```

VETTORI MULTIDIMENSIONALI

I vettori esaminati finora sono stati di tipo monodimensionale, ovvero si possono immaginare come pile di elementi navigabili attraverso un solo valore (l'indice).
È ovviamente possibile in qualsiasi linguaggio di programmazione dichiarare vettori a più dimensioni, anche se in genere non si va oltre alle due dimensioni e raramente si usano vettori a tre dimensioni (il loro uso può per esempio capitare in applicazioni scientifiche che debbano gestire dei tensori).
Un vettore a due dimensioni (multidimensionale) viene anche detto matrice e gli elementi al suo interno si esplorano usando due indici al posto di uno. Concettualmente una matrice si può immaginare come una tabella dotata di righe e colonne.
Per accedere a un determinato elemento, bisognerà fornire il suo indice di riga e il suo indice di colonna.

La dichiarazione anche in questo caso è molto semplice. Per una matrice di 10 righe e 10 colonne (10x10):

```
int matrice[10][10];
```

Da cui offriamo la seguente, più generale:

DEFINIZIONE 22
DICHIARAZIONE DI UN ARRAY MULTIDIMENSIONALE

Un array (vettore) multidimensionale in C si dichiara mediante la seguente forma: <tipo> <nome>[< righe>][< colonne>]; .

L'inizializzazione "statica" sarà invece qualcosa del tipo:

```
int matrice[3][3] = {
      { 1,2,3 },
      { 2,4,6 },
      { 3,6,9 }
};
```

Vediamo subito un applicativo molto semplice che esegue la somma di due matrici A e B collocando il risultato in una terza matrice C (la somma di due matrici è una matrice costruita in modo che C[i][j] = A[i][j] + B[i][j]):

```
#include <stdio.h>

#define   MAX_ROWS      10
#define   MAX_COLS      10

int main() {
      int i,j;
      int rows, cols;
      float A[MAX_ROWS][MAX ¬
_COLS], B[MAX_ROWS][MAX_COLS], ¬
C[MAX_ROWS][MAX_COLS];

      do {
            fprintf (stdout, "Inserire
il numero di righe e colonne delle matrici
nel formato \"righe,colonne\" "
                  "(max. righe:
%d, max. colonne: %d)\n", MAX_ROWS,
MAX_COLS);
            scanf ("%d,%d",
&rows, &cols);
      } while ( (rows < 0 || rows > MAX_ ¬
ROWS) && (cols < 0 || cols > MAX_COLS) );

      for (i=0; i < rows; i++) {
            for (j=0; j < cols; j++) {
                  fprintf ¬
(stdout, "A[%d][%d]: ", i+1, j+1);
                  scanf ("%f", ¬
&A[i][j]);

                  fprintf ¬
(stdout, "B[%d][%d]: ", i+1, j+1);
                  scanf ("%f", ¬
&B[i][j]);
            }
      }

      for (i=0; i < rows; i++) {
            for (j=0; j < cols; j++) {
                  C[i][j] = ¬
A[i][j]  + B[i][j];
                  fprintf ¬
(stdout, "C[%d][%d]: %f\n", i+1, j+1, C[i][j]);
            }
      }

      return 0;
}
```

Si noti l'uso dei due indici (i e j) per accedere alle locazioni all'interno delle matrici.

RICERCA LINEARE

Una delle operazioni più frequenti compiute sui vettori è ricercare elementi all'interno di questi ultimi.
Si comprende che la ricerca, essendo un'operazione così comune, è anche cruciale, in quanto un buon algoritmo di ricerca garantisce buone prestazioni algoritmiche complessive, specie in programmi di una certa complessità (Definizioni 8, 9 e 10 - HJ 201). Il tipo di ricerca più semplice (ma tuttavia funzionante) in un vettore è quella lineare. Semplicemente, l'algoritmo parte dall'inizio del vettore e comincia a scorrerlo elemento per elemento, fermandosi quando l'elemento viene trovato oppure quando viene raggiunta la fine del vettore. Come cercare un documento nell'archivio di prima partendo dalla cima e scorrendo tutti i cassetti in ordine.
Di seguito una implementazione esemplificativa (la funzione "search" ritorna -1 se il valore non è trovato, altrimenti l'indice a cui il valore è stato trovato, nel caso in cui ci siano più istanze di quel valore trovate nell'array sarà ritornato solo il primo):

ALGORITMO 1
RICERCA LINEARE

```
int search (int elemento, int
vettore[], int dimensione)  {
      int i;

      for (i=0; i < dimensione; i++)  {
            if (vettore[i] == elemento)
                  return i;
      }

      /* Se arriviamo qui, il ciclo sul
vettore è finito,
       * quindi l'elemento non è
stato trovato e ritorniamo -1*/
      return -1;
}
```

Si noti il passaggio di vettore alla funzione con le parentesi quadre [] per identificarlo come vettore e distinguerlo in tal modo dalle variabili scalari.

Di seguito un esempio di applicazione:

```
#define   SIZE      5
...
int index;
int v[] = { 0,1,2,3,4 };
...
/* Controllo se il vettore contiene il valore 2 */
index = search(2, v, SIZE);

if (index >= 0)
          fprintf (stdout, "Valore trovato in posizione %d nel vettore\n", index);
else
          fprintf (stdout, "Valore non trovato\n");
```

Si nota immediatamente che, nel caso migliore (elemento da cercare presente in prima posizione), l'algoritmo termina al primo colpo.
Nel caso peggiore (elemento da cercare presente all'ultima posizione o non presente), l'algoritmo esamina tutti gli elementi del vettore prima di terminare, quindi compie n iterazioni.
Nel caso medio, l'algoritmo compierà n/2 iterazioni prima di terminare.
La complessità algoritmica è quindi O(n), ed è per questo che tale algoritmo di ricerca viene definito lineare.
Dovrebbe ora risultare decisamente più chiara l'analisi tesa ad individuare le operazioni che rappresentano il procedimento dominante dell'algoritmo vista nel corso della scorsa parte.

RICERCA BINARIA

È dimostrabile che l'algoritmo di ricerca binaria non è sempre il migliore possibile per trovare un valore all'interno di un vettore.
Se il vettore non è ordinato, è naturalmente l'unico algoritmo possibile, in quanto non conoscendo l'ordine in cui gli elementi sono disposti possiamo solo esaminarli tutti prima di dire se un elemento c'è o meno. Ma se il vettore è ordinato, è possibile eseguire un algoritmo di ricerca più raffinato noto come ricerca binaria o ricerca dicotomica. Il principio è molto semplice e molto simile a quello che si fa, ad esempio, quando si vuole cercare un nome nell'elenco telefonico. Essendo l'elenco telefonico già ordinato in modo alfabetico, infatti, l'approccio più conveniente quando si deve cercare un nome non è quello di partire dall'inizio e scorrere tutti i nomi finché non si trova quello desiderato. Un buon metodo di ricerca può essere quello di aprire l'elenco nel mezzo, controllare se il nome da cercare inizia con una lettera che sta prima o dopo quella associata alla pagina aperta, e, rispettivamente, andare a cercare il nome nella metà precedente o nella metà successiva.
Si ripete quindi l'algoritmo finché il valore non viene trovato, oppure finché gli indici inizio-fine dei sotto-vettori non si invertono (in tal caso, abbiamo già esaminato tutto il sotto-vettore, quindi il valore non è stato trovato).
Vediamo un semplice esempio di applicazione:

```
#define   SIZE      8
...

int v[] = { 1,1,2,3,5,8,13,21 }
int index;
...

index = search(3, v, SIZE);

if (index >= 0)
          fprintf (stdout, "Valore trovato in posizione %d\n", index);
else
          fprintf (stdout, "Valore non trovato\n");
```

Ovviamente, ancora una volta, l'ipotesi sotto la quale un algoritmo di ricerca binaria può funzionare è che il vettore sia ordinato. Se non si ha questa sicurezza, è opportuno prima ordinare il vettore attraverso un algoritmo di ordinamento, quindi operare la ricerca.
È dimostrabile che, mentre la ricerca lineare ha una complessità computazionale nell'ordine di O(n), la ricerca binaria ha una complessità nell'ordine di O(log n), ovvero una complessità logaritmica contro una lineare.
Questo vuol dire che, se il vettore ha 256 elementi, un algoritmo di ricerca binaria potrebbe compiere al più 8 iterazioni nel caso peggiore, mentre quello lineare ne compierà 256.

ALGORITMI DI ORDINAMENTO

L'ordinamento è uno dei momenti più ricorrenti nella logica di un software.
Lo stesso computer in francese viene chiamato ordinateur, il che lascia intuire che l'ordinamento è una delle funzioni principe di un algoritmo.

ALGORITMO 2
RICERCA DICOTOMICA

1. Si parta da un vettore v, all'interno del quale si vuole cercare un valore x, partendo dall'indice start=0 e arrivando all'indice end=dim-1, dove dim è la dimensione di v.
2. Selezioniamo l'elemento mediano (pivot o sentinella) del vettore, ovvero v[(start+end) / 2].
3. Se start > end, allora abbiamo esaminato tutto il sottovettore, quindi ritorniamo -1, non avendo trovato il valore.
4. Se v[pivot] = x, allora il valore di sentinella è proprio quello che cercavamo, quindi ritorniamo alla sua posizione.
5. Se v[pivot] > x, allora, essendo il vettore ordinato, dato che il valore di sentinella è più grande di quello che cerchiamo, il valore x, se c'è, dovrà stare nella metà che precede pivot, quindi richiamiamo la funzione sul sotto-vettore che va da start a pivot-1.
6. Se v[pivot] < x, allora x, se esiste, sarà nella metà che succede pivot, quindi richiamiamo la funzione sul sotto-vettore che va da pivot+1 a end.

```
int search (int elemento, int vettore[], int start, int end)  {
      int pivot = (start+end)/2;

      if (start > end)
            return -1;
      else if (vettore[pivot] == elemento)
            return pivot;
      else if (vettore[pivot] > elemento)
            return search (elemento, vettore, ¬
start, pivot-1);
      else
            return search (elemento, vettore, ¬
pivot+1, end);
}
```

Proprio per questo si sono sviluppati algoritmi di ordinamento via via più sofisticati, per rendere minimo l'impatto computazionale ed in tal modo ottimizzare le prestazioni complessive del programma. In questa sede esamineremo l'algoritmo di ordinamento detto di bubble sort e quello più ottimizzato detto quick sort.

BUBBLE SORT

Il bubble sort non è l'algoritmo più efficiente (la sua complessità computazionale è nell'ordine di $O(n^2)$, mentre algoritmi come quick sort e merge sort arrivano a O(n log n)) ma probabilmente il più intuitivo da capire e riprodurre.

ALGORITMO 3

BUBBLE SORT

1. Sia dato un vettore v di dimensione dim.
2. Si parta dall'ipotesi che v sia ordinato.
3. Cicliamo su tutti gli elementi del vettore.
4. Se per un generico i si ha che v[i] > v[i+1], ovvero ci sono due elementi consecutivi di cui il primo è più grande del secondo (quindi l'array non è ordinato), scambieremo fra di loro questi due elementi marcando il vettore come "non ordinato".
5. Ripeteremo finché il vettore non è definitivamente ordinato.

```
void sort (int v[], int dim)  {
        int i, sorted;

        do  {
        sorted = 1;

        for (i=0; i < dim-1; i++)  {
            if (v[i] > v[i+1])  {
                v[i] ^= v[i+1];
                v[i+1] ^= v[i];
                v[i] ^= v[i+1];
                sorted = 0;
            }
        }
    } while (sorted == 0);
}
```

La variabile sorted è una specie di variabile di stato il cui contenuto è interrogato di volta in volta per verificare lo stato del vettore. Si notino le tre righe subito dopo l'if (Definizione 11 - HJ 201).

Queste fondamentalmente scambiano fra di loro i valori contenuti in v[i] e v[i+1] usando un piccolo stratagemma logico (l'operatore ^ è quello di XOR, o OR esclusivo, che opera su due bit per volta e ritorna 1 se i due bit sono diversi e 0 se sono uguali, allo stesso modo scrivere x ^= y equivale a scrivere x = x ^ y).

È un modo raffinato per scambiare fra loro due valori, senza usare variabili ausiliarie. Il modo comunemente accettato, infatti, prevede di usare una terza variabile temporanea per salvare il valore intermedio ed evitare che venga così cancellato dalla sovrascrittura. Ad esempio, per scambiare a e b:

```
int a,b,tmp;
...

tmp = a;
a = b;
b = tmp;
```

Il metodo illustrato invece nell'algoritmo di sort fa in modo che non sia necessario usare una terza variabile.

Per i più bravi, potete cimentarvi nel capire in che modo quelle tre righe operano lo scambio, e proporre eventuali soluzioni sul nostro forum (www.hackerjournal.it). Quando parleremo di puntatori sarà anche chiaro come scrivere una funzione che operi lo scambio.

Per ora, si può notare come il valore di ritorno della funzione sia void (ovvero non ritorni niente) e ciononostante il vettore risulti modificato. Questo, detto un po` grossolanamente, accade perché quando si passa un vettore ad una funzione non si passa il suo valore, ma il suo indirizzo di memoria, tutte le modifiche sono effettuate lì risultando quindi visibili anche qualora la funzione fosse terminata. Questi concetti risulteranno più semplici da comprendere quando introdurremo i puntatori.

QUICK SORT

Il quick sort è un algoritmo in loco (o in place, vedi richiamo teorico 5) di ordinamento piuttosto ottimizzato ideato da Charles A. Richard Hoare nel 1961 ed è l'algoritmo di ordinamento implementato nella libreria standard del C (funzione qsort() in stdlib.h, mentre altri linguaggi, come Java e Perl, implementano di default il merge sort come algoritmo di ordinamento). Si dimostra che nel caso medio quest'algoritmo è in grado di ordinare un vettore di dimensione n operando un numero di confronti nell'ordine di O(n log n).

Il funzionamento dell'algoritmo (che è ricorsivo - vedi richiamo teorico 6) è del tipo divide et impera, ovvero divide il vettore di partenza in sottovettori man mano più piccoli, ordinando gli elementi al loro interno, per poi ordinare i sottovettori già ordinati, risalendo fino ad ottenere il vettore di partenza ordinato (si perdoni il gioco di parole).

RICHIAMO TEORICO 5

ALGORITMI IN LOCO.
Un algoritmo è denotato come in loco (o in place) se è in grado di svolgere le proprie operazione elaborative senza occupare uno spazio di memoria eccedente rispetto alla dimensione dell'input di dati iniziali oppure ne occupa una minima parte costante.

RICHIAMO TEORICO 6

ALGORITMI RICORSIVI.
Il concetto di ricorsione nella progettazione del software è comunemente (e spesso erroneamente) implementato attraverso l'utilizzo di funzioni. Risulta quindi evidente che scrivere e disporre di algoritmi iterativi (ovvero che l'esecuzione su un insieme N di dati si traduca nell'applicazione ripetuta dello stesso algoritmo andando di volta in volta a suddividere l'insieme di partenza in insiemi più piccoli e quindi meno complessi) rivesta molta importanza.
Un tipico esempio di algoritmo ricorsivo è, per l'appunto, il Quick Sort.

ALGORITMO 4

QUICK SORT

1. Sia dato un vettore v di dimensione n, con elementi i cui indici vanno da 0 a n-1.
2. Se il vettore è vuoto, interrompiamo l'esecuzione.
3. Individuiamo l'elemento intermedio del vettore, o "sentinella", in posizione n/2.
4. Controlliamo che tutti gli elementi a sinistra della sentinella siano minori di essa e quelli a destra maggiori.
5. Se così non fosse, scambieremo il valore fuori posto con uno a sinistra o a destra della sentinella, a seconda che il valore fuori posto sia maggiore o minore, in modo da portarlo nel sottovettore giusto.
6. Richiamiamo il quick sort sulla metà sinistra del vettore.
7. Richiamiamo il quick sort sulla metà destra del vettore.

```
void sort( int *v, int first, int last
) {
        int i,j,pivot;

        if (first < last)  {
                i=first; j=last;
                pivot=v[(first+last)/2];

                while (v[i]<pivot) ¬
i++;
                while (v[j]>pivot)      j--;

                if (i<=j)  {

                        v[i] ^= v[j];

                        v[j] ^= v[i];

                        v[i] ^= v[j];

                        i++; j--;
                }

                sort(v,first,j);
                sort(v,i,last);
        }
}
```

Che invocheremo come:

```
int v[SIZE];
...
sort (v, 0, SIZE-1);
```

PASSARE AI PUNTATORI

In realtà, i termini "array" e "vettore" in C rispondono unicamente ad un'esigenza di tipo "grammaticale" di dover definire un'apposita struttura dati preposta a contenere determinati valori in un ben definito modo.

Infatti, attraverso la dichiarazione di un array in C implicitamente dichiariamo un puntatore che referenzia l'area di memoria che ospiterà i predetti valori. Non è quindi un caso che questa parte del Corso serva da biglietto da visita per quella destinata unicamente ai puntatori.

Questo, volendo commettere un abuso linguistico giustificato dal fatto di permettere una precisa cognizione di quanto sviluppato in questa sede, a dimostrazione del fatto che, all'interno della macchina informatica e precisamente in C la stessa definizione di array come "dato strutturato" poggia le basi su un complesso meccanismo gestito a sua volta da più entità "atomiche".

È una sfumatura, per certi versi, decisamente "filosofica" e poco "tecnica" ma che ben evidenzia un certo grado di astrazione funzionale e logica, da considerarsi come una condicio sine qua non per qualsiasi aspirante programmatore in quanto estrinseca nel migliore dei modi i meccanismi e le modalità di ragionamento edificanti per il neonato developer.

Torniamo per un attimo all'esempio proposto prima:

```
int miovettore[10];
```

All'atto di questa dichiarazione, le operazioni svolte dal Calcolatore (per le quali, ora, ometteremo un eccessivo terminismo e tecnicismo) si possono riassumere come segue:

1. Allocazione di memoria per una locazione di memoria costante identificata dal nome "miovettore".
2. Allocazione di memoria per dieci valori di tipo intero direttamente legati all'etichetta "miovettore".
3. Inizializzazione di quanto referenziato da "miovettore" con l'indirizzo di memoria puntato dal primo valore dei dieci.

Si provi, per ora assumendolo per partito preso, a dichiarare l'array di prima come di seguito e ad utilizzare gli stessi cicli visti prima per riempirlo e stampare a video i valori:

```
#include <stdio.h>
#include <stdlib.h>

int main()
{
        int i;

        // sostituiamo int miovettore[10]
con:
        int *miovettore;
        miovettore = (int*)
malloc(10*sizeof(int));

        for (i=0; i < 10; i++) {
                fprintf (stdout, "Ele-
mento n.%d: ", i+1);
                scanf ("%d",
&miovettore[i]);
        }

        for (i=0; i < 10; i++)
                fprintf (stdout, "L'ele-
mento n.%d vale %d\n", i+1, miovettore[i]);

}
```

LA COMPILAZIONE

Compilando e mandando in esecuzione il programma il lettore si accorgerà autonomamente che il funzionamento non è minimamente mutato:

```
$ gcc test.c -o test
$ ./test
Elemento n.1: 1
Elemento n.2: 2
...
Elemento n.10: 10

L'elemento n.1 vale 1
L'elemento n.2 vale 2
...
L'elemento n.10 vale 10
```

A rispondere ai come, ai se, ai ma ed ai perché ci penserà la quarta parte del Corso. Alla prossima!

Massimiliano Rinaldi
redazione@hacker journal.it

FTP_BT

IL CANALE DI ATTACCO È SERVITO!

MOBILE
VOLETE "COMANDARE" VIA BLUETOOTH IL TELEFONO DI UNA VITTIMA INCONSAPEVOLE? FTP_BT È QUELLO CHE FA AL CASO VOSTRO...

Qualche numero fa abbiamo trattato Blooover (proprio con tre "o", una delizia per il correttore bozze...) che ha incontrato il favore dei lettori. Proprio uno di essi (è giusto dare a Cesare quello che è di Cesare) ci ha segnalato un software similare, sempre scritto in java, disponibile su internet, Ftp_bt all'indirizzo HYPERLINK "http://www.ismuka.com/01/02/guida-a-ftp_bt-o-bt_info.html" http://www.ismuka.com/01/02/guida-a-ftp_bt-o-bt_info.html. Le segnalazioni dei nostri lettori sono spesso utili, a volte sacre, abbiamo quindi deciso di testare questo piccolo applicativo del peso di pochi kb (100)

Le affinità con Blooover sono diverse, solo che mentre Blooover si rivela efficace nell'attaccare soprattutto cellulari Nokia , questo software si concentra su gran parte dei Motorola, che sono particolarmente vulnerabili, Sony Ericsson ed LG. Diciamo che per certi versi i due software si possono anche considerare complementari, dove non arriva l'uno può arrivare l'altro.

TECNICHE DI HACKING

La tecnica per entrare e comandare il cellulare vittima è la stessa utilizzata da molti programmi similari attraverso il canale Bluetooth con l'invio al cellulare vittima, di un messaggio di accettazione di questo tipo: "Accettare richiesta di connessione da –nome cellulare-".
Infatti, per potere esplicare il "suo potere" è necessario che il cellulare oggetto di attacco accetti la connessione. E' un po' come il vampiro che ha bisogno di essere invitato in casa dalla vittima altrimenti non può varcare la soglia...
Fatto questo si può utilizzare Ftp_bt per:

- leggere i messaggi (del telefono vittima)
- leggere la rubrica
- modificare la rubrica
- vedere alcune info sul telefono
- spegnere il telefono
- cambiare modo d'uso
- farlo squillare
- farlo chiamare
- chiamare un numero attraverso quel telefono
- premere i tasti
- vedere i tasti premuti
- formattarlo

PROVA SU STRADA

La prima operazione da fare è quella di scaricare Ftp_bt e di installarlo sul cellulare attaccante

via Pc (con cavo o attraverso il Bluetooth).
Una volta caricato l'installer ftp_bt_1.08.jar si può procedere all'installazione vera e propria del pacchetto sul cellulare (ignorando gli avvisi di protezione che compariranno).
Una volta installato troverete un'icona ftp_bt nella cartella Applicazioni o similari del vostro cellulare. Lanciate l'applicazione.
Alla prima apertura il programma vi chiederà di selezionare la lingua. L'unica comprensibile tra quelle proposte è l'inglese, occorre scorrere tutte le lingue proposte fino ad arrivare alla sezione relativa alla scelta della lingua Jazik>Slovencina. Cliccate. Dovrebbe comparire un menu da cui è possibile selezionare la lingua inglese, volendo anche il tedesco.

Tornate al menu principale selezionando informàcie (nel Nokia dal menu Opzioni).

Comparirà un menu con 4 voci:

Connect
Setting
About
Exit

La voce che ci interessa è Connect. Selezionatela e subito dopo scegliete inquiry devices. il programma cercherà tutte le periferiche bluetooth nel suo raggio d'azione (circa 100 metri). Scegliete una delle periferiche. Se la periferica vittima accetta la richiesta di connessione il gioco è fatto. Il programma si chiama ftp perché infatti non fa nient'altro che aprire una sorta di canale dati che peraltro necessita della cortese attivazione anche da parte della vittima.

L'invio degli attacchi avviene proprio attraverso questo canale "preferenziale"...

ALL'ATTACCO

A questo punto non resta che selezionare la tecnica di attacco tra quelle suggerite.
Ad esempio per spegnere un Nokia 6600 basta andare nella schermata Phone Functionality Selzionare Minimum Functionality e il telefono si spegne. Per i Motorola si accede alla schermata Custom Command si va su Turn Off Phone(SE) e senza premere niente altro, si preme il pulsante sinistro (Options).
Bisogna entrare nel menu Edit Command e aggiungere nel campo Command uno 0 in fondo (trasformando il 10 in 100).
Quindi basta Premere su Select e attendere. Premendo nuovamente su Select il telefono si spegnerà.

Si consideri il seguente testo cifrato con un Algoritmo da noi inventato
(si utilizzino gli esempi proposti per capire il funzionamento).

Suggerimento: L'algoritmo è applicato ad ogni singolo carattere della frase proposta, spazi esclusi. L'alfabeto utilizzato è quello inglese.

Esempi:
CIAO = DJGLODWNKKQUHI
MISS = NKGUAVZYXOJRET

TXMMZQYLIPLIABTGMZUVLIOENTYUBOLXZOESXLACMUXJCXLIEAZBDJYBIEQDJSTXLTXACEXSSONDU
QUDTQCSSXNVUJLHACKERJOURNALNXNTUCLTVXYJZQATLAEQCSSXNDUDTQQBADCVXJTOYYYDTQQ
QVKGJFLDKRITJGKFLDKVAUEMVHDKFJGLEOTUFJBAJSYTALPFHGKECBAMFSMKEHGJFOEPSAM
CXJGKELDHAUTPQLGKFJBMVNAHFJKGLMHGJFKDLTKRMGJFKDLROQPV

Newbie: si risalga al testo in chiaro della frase.
Mid: si scriva un applicativo capace di decifrare testi che utilizzano questo AR.
Esperti: si scriva un applicativo capace di cifrare e decifrare testi utilizzando questo AR.

Inviate tutto a cyberenigma@hackerjournal.it specificando come oggetto della mail il livello (newbie/mid/esperti) ed il numero della rivista del cyberenigma risolto. I migliori saranno pubblicati in questa pagina e sul sito www.hackerjournal.it!